safend

a wave systems company

SAFEND Data Protection Suite™

Installation Guide

Version 3.4.5

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Important Notice

This guide is delivered subject to the following conditions and restrictions:

- ✓ This guide contains proprietary information belonging to Safend Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized Safend Data Protection Suite users.
- ✓ No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the expressed prior written permission of Safend Ltd.
- ✓ The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- ✓ The software described in this guide is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.
- ✓ Information in this guide is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- ✓ The information in this document is provided in good faith but without any representation or warranty whatsoever, whether it is accurate, or complete or otherwise and with the expressed understanding that Safend Ltd. shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.

Copyright ©2005-2011 Safend Ltd. All rights reserved.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

About This Guide

This Installation Guide is comprised of the following chapters:

- ✓ ***Chapter 1 Installation Workflow*****,** page 6, suggests a workflow for using the Safend Data Protection Suite solution to protect your organization's endpoints.
- ✓ ***Chapter 2 Preparing for Installation*****,** page 9, describes the Safend Data Protection Suite architecture and the Safend Data Protection Suite installation workflow. It then describes the system requirements and prerequisites for installation and all the preparations that need to take place before installing Safend Data Protection Suite.
- ✓ ***Chapter 3 Installing Safend Data Protection Suite Management Server*****,** page 12, describes how to install, restore and upgrade the Safend Data Protection Suite Management Server, and how to launch the Safend Data Protection Suite Management Console.
- ✓ ***Chapter 4 Installing Safend Data Protection Suite Management Console*****,** page 40, describes how to install Safend Data Protection Suite Management Console.
- ✓ ***Chapter 5 Installing Safend Data Protection Suite Client*****,** page 49, describes the various methods for installing, or deploying, Safend Data Protection Suite Client. It also explains how to uninstall and upgrade Safend Data Protection Suite Client.
- ✓ ***Chapter 6 Installing a MAC Client*****,** page 70, describes the procedure for installing and uninstalling a Mac client.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Table of Contents

Chapter 1 Installation Workflow 6
Safend Data Protection Suite Implementation Workflow 7

Chapter 2 Preparing for Installation 9
System Requirements 10
Preparing your Network 10
Opening WMI ports on Windows XP (SP2) Firewall 10
Tips on Preparing Your Endpoints 11

Chapter 3 Installing Safend Data Protection Suite Management Server 12
Prerequisites 13
Installing Prerequisite Software 13
Installing Microsoft .NET Framework 2.0 13
Installing Microsoft IIS 13
Before Installing Safend Data Protection Suite Management Server 15
Installing the Management Server 15
Restoring an Existing Management Server 28
Upgrading the Management Server 31
Considerations Before Performing Management Server Upgrade 31
Upgrading a Clustered Server Environment 36
Post-Installation Settings (Checklist) 37
Checklist for the Most Critical Settings in the Administration Window 37
Checklist for the Most Critical Settings in the Global Policy Settings Window 37
Uninstalling Safend Data Protection Suite Management Server 38
Changing your Database 38

Chapter 4 Installing Safend Data Protection Suite Management Console 40
Prerequisites 41
Installing Prerequisite Software 41
Installing Microsoft .NET Framework 2.0 41
Installing Safend Data Protection Suite Management Console 41
Installing the Console from the Installation Web Page 41
Installing Safend Data Protection Suite Management Console Manually 46

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Launching Safend Data Protection Suite Management Console for the First Time.... 47
Uninstalling Safend Data Protection Suite Management Console..... 48

Chapter 5 Installing Safend Data Protection Suite Client.....49
Prerequisites 50
Before Deploying Safend Data Protection Suite Client 50
Installing Safend Data Protection Suite Client 52
Automatic Client Installation (Active Directory) 52
Automatic Client Installation (Generic) 57
Manual Client Installation 57
Upgrading Safend Data Protection Suite Client..... 61
Considerations Before Performing Client Upgrade 61
Upgrading the Client via Active Directory 61
Upgrading the Client Manually 62
Uninstalling Safend Data Protection Suite Client..... 62
Uninstalling Manually 62
Uninstalling Safend Data Protection Suite via GPO 66
Safend Data Protection Suite Client Cleanup Utility 67
Emergency Agent Uninstall 67

Chapter 6 Installing a MAC Client 70
Prerequisites 71
Preparing the Installation Package 71
Installing a Safend Data Protection Suite Mac Client 71
Uninstalling a Safend Data Protection Suite Mac Client 76

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Chapter 1

Installation Workflow

About This Chapter

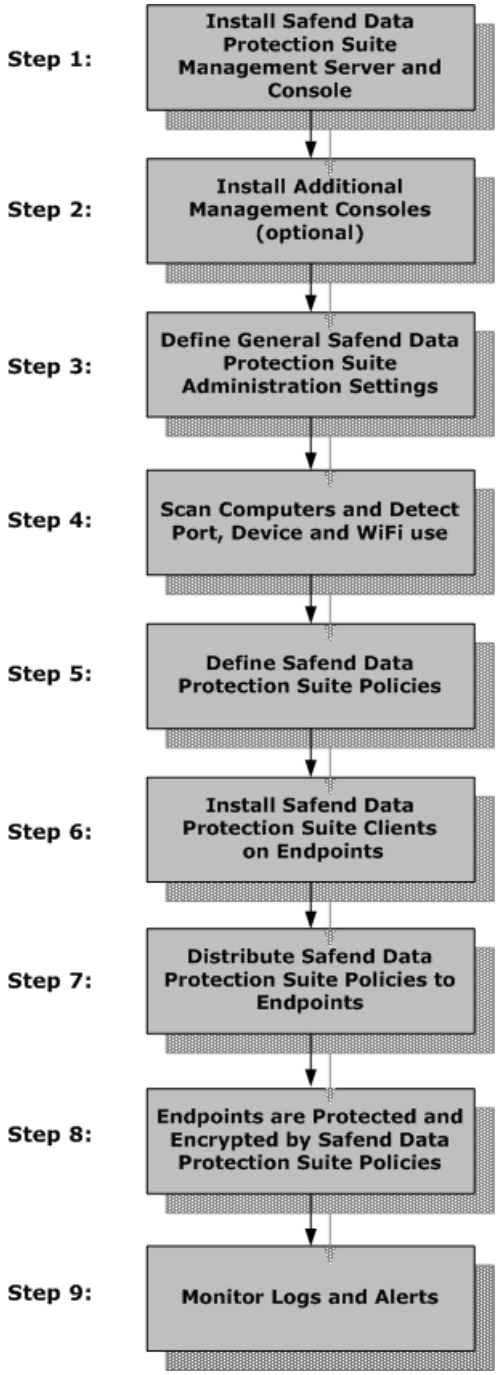
Before installing Safend Data Protection Suite V3.4, it is important to understand fully the implementation process of the Data Protection Suite solution. This chapter suggests a workflow for using the Safend Data Protection Suite solution to protect your organization's data. It contains the following section:

- ✓ ***Safend Data Protection Suite Implementation Workflow***, page 7 describes the workflow for implementing and using the Safend Data Protection Suite.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Safend Data Protection Suite Implementation Workflow

The following is an overview of the workflow for implementing and using Safend Data Protection Suite.


Step 1:
Install Safend Data Protection Suite Management Server and Console
Step 2:
Install Additional Management Consoles (optional)
Step 3:
Define General Safend Data Protection Suite Administration Settings
Step 4:
Scan Computers and Detect Port, Device and WiFi use
Step 5:
Define Safend Data Protection Suite Policies
Step 6:
Install Safend Data Protection Suite Clients on Endpoints
Step 7:
Distribute Safend Data Protection Suite Policies to Endpoints
Step 8:
Endpoints are Protected and Encrypted by Safend Data Protection Suite Policies
Step 9:
Monitor Logs and Alerts

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

- ✓ **Step 1: Install the Safend Data Protection Suite Management Server and Console**, as described in *Chapter 2 Preparing for Installation*, page 9 and *Chapter 3 Installing Safend Data Protection Suite Management Server*, page 12.
- ✓ **Step 2: Install Additional Management Consoles**, as described in *Chapter 4 Installing Safend Data Protection Suite Management Console*, page 40.
- ✓ **Step 3: Define General Safend Data Protection Suite Administration Settings,** such as the method in which policies are published, as described in *Chapter 12, Administration* in the *Safend Data Protection Suite User Guide*.
- ✓ **Step 4: Scan Computers and Detect Port, Device and WiFi Use**, Use Safend Auditor to detect the ports that have been used in your organization and the devices and WiFi networks that are or were connected to these ports, as described in the *Safend Auditor User Guide*.
- ✓ **Step 5: Define Safend Data Protection Suite Policies,** In this stage you define the blocked, allowed and restricted ports, devices and WiFi networks according to the security and productivity requirements of your organization as described in the *Safend Data Protection Suite User Guide*.
- ✓ **Step 6: Install Safend Data Protection Suite Clients on Endpoints,** as described in *Chapter 5 Installing Safend Data Protection Suite Client*, page 49.
- ✓ **Step 7: Distribute Safend Data Protection Suite Policies to Endpoints,** in this stage, you can either associate policies to users and computers and distribute them directly to endpoints (via SSL), or use Active Directory's GPO feature to distribute Safend Data Protection Suite Policies or any other third-party tool, as described in the *Safend Data Protection Suite User Guide*.
- ✓ **Step 8: Endpoints are Protected and Encrypted by Safend Data Protection Suite Policies**, in this stage, only approved devices and WiFi networks can be used, through permitted ports. Logs about port, device and WiFi network use and attempted use, as well as tampering attempts, are created and sent to the Management Server as described in the *Safend Data Protection Suite User Guide*.
- ✓ **Step 9: Monitor Logs and Alerts,** view and export the log entries generated by Safend Data Protection Suite Clients, as described in *Chapter 10, Viewing Logs* in the *Safend Data Protection Suite User Guide.*

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Chapter 2

Preparing for Installation

About This Chapter

This chapter first describes the Safend Data Protection Suite architecture and the Safend Data Protection Suite installation workflow. It then specifies the system requirements and prerequisites for installing the different components of the Safend Data Protection Suite, followed by instructions on how to prepare the network for installation. It contains the following sections:

- ✓ ***System Requirements***, page 10, describes the system requirements for each one of the Safend Data Protection Suite components.
- ✓ ***Preparing your Network***, page 10, describes the preparations that need to be made on your network in order to allow the different Safend Data Protection Suite components to communicate without interruptions.
- ✓ ***Tips on Preparing Your Endpoints***, page 11, describes the preparation that needs to be made on your endpoints before installing Safend Data Protection Suite in order to optimize the security of your network.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

System Requirements

NOTE

Refer to the *What's New* document for the most up-to-date system requirements.

Preparing your Network

Before installing the system, be sure to enable the following communications in your network and personal firewalls.

➢ **To prepare your network:**

1. In order to communicate freely between the Safend Data Protection Suite Management Server and the Safend Data Protection Suite Clients, make sure that the SSL port is open in your network firewall. Safend typically uses port 443 (SSL standard) for this. If you have chosen otherwise, make sure to allow this port in your firewall.
2. In order for the Safend Data Protection Suite Management Console to be able to control clients (send control commands to clients to send their logs and update their policy), it needs WMI ports to be open on the personal firewalls of each endpoint. WMI uses port 135 and a series of random ports.

Opening WMI ports on Windows XP (SP2) Firewall

If you are using Windows XP (SP2) firewall as the personal firewall on your endpoints, you can use the GPO mechanism to configure endpoints to accept incoming WMI communications. The following section is a quote from the Microsoft documentation.

"Without configured exceptions, Windows Firewall will drop traffic for server, peer, or listener applications and services. Therefore, it is likely you will want to configure Windows Firewall for exceptions to ensure that the Windows Firewall works appropriately for your environment. Windows Firewall settings are available for Computer Configuration only".

They are located in **`Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall`**.

Identical sets of policy settings are available for two profiles:

- ✓ Domain profile. Used when computers are connected to a network that contains your organization's Active Directory domain.
- ✓ Standard profile. Used when computers are not connected to a network that contains your organization's Active Directory domain, such as a home network or the Internet.

The relevant policy setting for WMI is:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Windows Firewall: Allow remote administration exception.
This allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using RPC and DCOM.
The default is "Not Configured".

Tips on Preparing Your Endpoints

Booting via an external boot device (floppy, CD, etc.) will circumvent any security software. However, there are a few ways to either prevent this scenario from happening, or make it impossible to be able to read the data outside the Safend protected operating system:

1. **Changing the boot sequence:** Change the boot sequence so that the machine does not boot first from the floppy, then the CD\DVD-ROM, and finally, the hard disk drive. The hard disk drive should always be the first boot device. If the floppy or the CD\DVD-ROM is the initial boot device, anyone can use a bootable medium that can directly access the hard disk drive and reset the administrator password in seconds.
2. **Physical seal\chassis protection:** Make sure that the hardware is sealed and that the hard disk drive cannot be simply disconnected.
3. **Setting a password to protect the BIOS:** This prevents users from entering the BIOS and re-enabling the boot access through devices other than the internal hard disk drive.
4. **Internal Hard Disk Encryption:** Safend Data Protection Suite includes the internal hard disk encryption feature – the Safend Encryptor. The Encryptor client encrypts all internal hard-drives, protecting data stored on them and makes sure that the data can be accessed only with the proper credentials. Trying to circumvent the normal booting sequence by booting from any external boot device will prove unsuccessful, since data can be decrypted only with the Safend Encryptor Client.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Chapter 3

Installing Safend Data Protection Suite Management Server

About This Chapter

This chapter describes how to install the Safend Data Protection Suite Management Server and contains the following sections:

- ✓ ***Prerequisites***, page 13, describes the requirements for installing the Management Server.
- ✓ ***Installing Prerequisite Software***, page 13, describes how to install Microsoft .NET framework and IIS.
- ✓ ***Before Installing Safend Data Protection Suite Management Server***, page 15, provides a checklist of issues you need to verify before starting the installation process.
- ✓ ***Installing the Management Server***, page 15, describes how to install the Safend Data Protection Suite Management Server for the first time and how to launch the Safend Data Protection Suite Management Console.
- ✓ ***Restoring an Existing Management Server***, page 28, describes how to restore an existing Safend Data Protection Suite Management Server in case of hardware upgrade or failure.
- ✓ ***Upgrading the Management Server*** page 31, describes how to upgrade the Management Server.
- ✓ ***Uninstalling Safend Data Protection Suite Management Server***, page 38, explains how to uninstall Safend Data Protection Suite Management Server.
- ✓ ***Changing your Database***, page 38, explains how to switch from using an embedded Safend Data Protection Suite database to an external MS SQL database, and vice versa.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Prerequisites

NOTE

Refer to the *What's New* document for the most up-to-date system requirements.

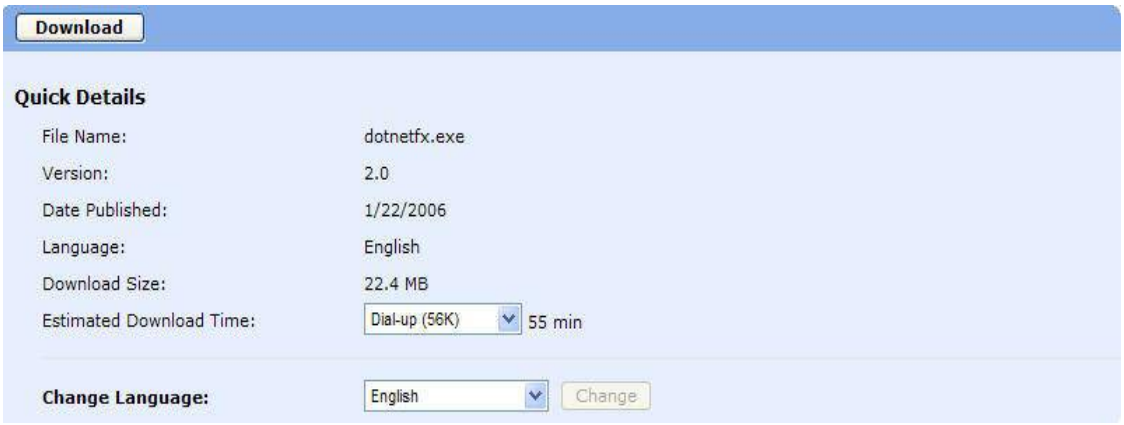
Installing Prerequisite Software

Installing Microsoft .NET Framework 2.0

➢ To install .NET Framework

Microsoft .NET Framework 2.0 is built in by default on Windows 2003, and can be downloaded for free from the Microsoft website for Windows XP.

The link to the .NET framework 2.0 installation package:
http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en



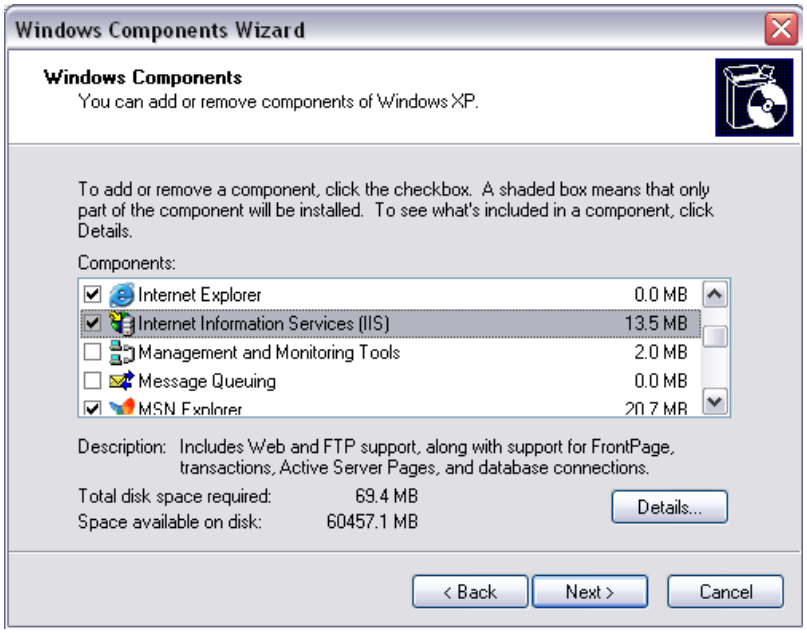
Installing Microsoft IIS

➢ To install Microsoft IIS:

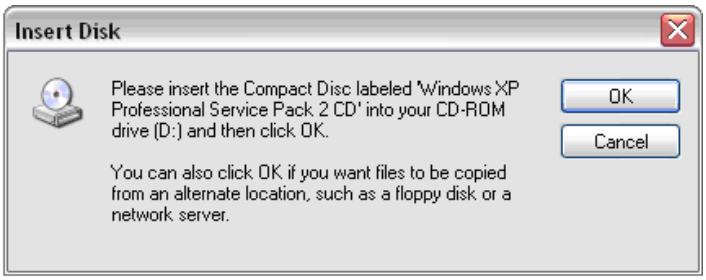
1. In the Control Panel on your computer, double-click **Add or Remove Programs**. The *Add or Remove Programs* window opens.
2. Click **Add/Remove Windows Components**. The Windows Components Wizard window opens.

   If you are installing the application on a machine running Windows 2003, check the *Application Server* checkbox**.** If you are installing IIS on a machine running Window XP, check the *Internet Information Services (IIS)* checkbox, as shown below:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Internet Explorer 0.0 MB
Internet Information Services (IIS) 13.5 MB
Management and Monitoring Tools 2.0 MB
Message Queuing 0.0 MB
MSN Explorer 20.7 MB
Description: Includes Web and FTP support, along with support for FrontPage, transactions, Active Server Pages, and database connections.
Total disk space required: 69.4 MB
Space available on disk: 60457.1 MB
Details...
< Back
Next >
Cancel

3. Click **Next**.
   The *Insert Disk* window opens, asking for the utility disc or location that holds the relevant Microsoft Windows installation components.


Insert Disk
Please insert the Compact Disc labeled 'Windows XP Professional Service Pack 2 CD' into your CD-ROM drive (D:) and then click OK.
You can also click OK if you want files to be copied from an alternate location, such as a floppy disk or a network server.
OK
Cancel

4. Insert the disc and click **OK.** The installation may take a few moments.
   When the wizard notifies you that the installation is complete, as shown in the following figure, click **Finish** to close the wizard. Microsoft IIS is now installed.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Windows Components Wizard
Completing the Windows Components Wizard
You have successfully completed the Windows Components Wizard.
To close this wizard, click Finish.
< Back
Finish

Before Installing Safend Data Protection Suite Management Server

Before installing the Management Server check the following:

1. Verify that all system requirements and prerequisites are met.
2. Make sure that the Safend Data Protection Suite Server machine belongs to the same domain in which you intend to deploy Safend Data Protection Suite policies.
3. Make sure that a MySQL DB is not installed on the Safend Data Protection Suite Management Server machine.

Installing the Management Server

Here is the procedure to follow when installing the Management Server.

➢ To install Safend Data Protection Suite Management Server:

1. Locate *SafendDataProtectionSuite.exe* on your installation CD.
2. Double-click the file. The *Safend Data Protection Suite Management Server* installation window is displayed.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Safend Data Protection Suite
Press Install button to start extraction.
Use Browse button to select the destination folder from the folders tree. It can be also entered manually.
If the destination folder does not exist, it will be created automatically before extraction.
Destination folder
C:\temp
Browse...
Installation progress
Install
Cancel

3. Click **Browse** to select a destination folder for the extracted installation files.

NOTE

Make sure that the files are extracted to a local folder. The installation will not run from a network path.

4. Click **Install**.

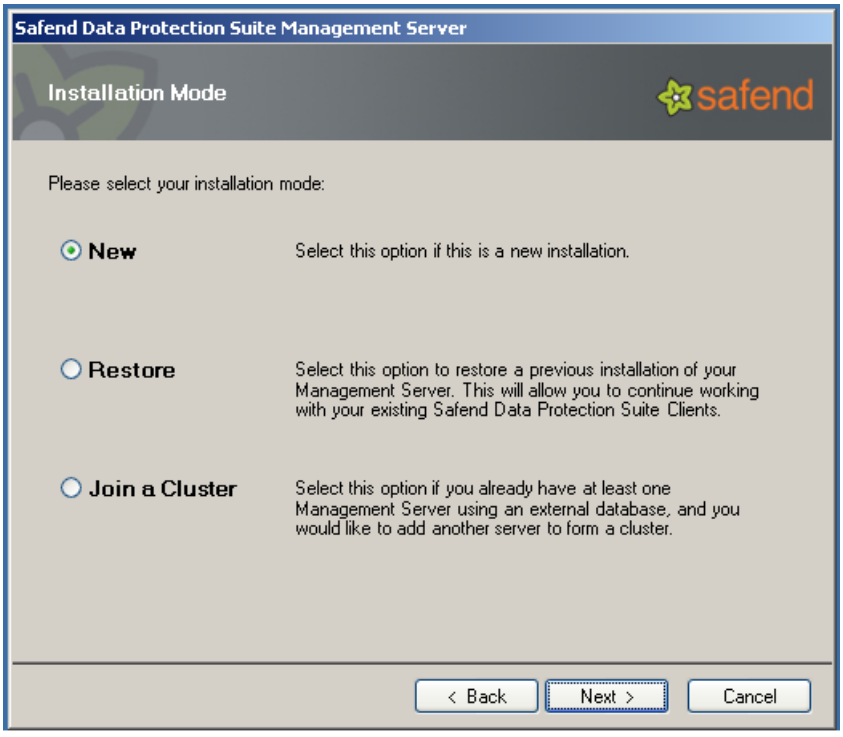
5. Following extraction, you will be asked to select the Safend Data Protection Suite Server language, as shown below:

6. Select the required language and click **OK**. The first step of the installation wizard is displayed.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Safend Data Protection Suite Management Server
SAFEND
Management Server
This wizard will install Safend Data Protection Suite Management Server on your computer.
Warning: This program is protected by copyright law and international treaties.
safend
Click Next to continue or Cancel to exit.
< Back
Next >
Cancel

7. Click **Next** and read the *End User License Agreement*. After accepting, click **Next** again. The *Installation Mode* window is displayed.


Safend Data Protection Suite Management Server
Installation Mode
safend
Please select your installation mode:
New
Select this option if this is a new installation.
Restore
Select this option to restore a previous installation of your Management Server. This will allow you to continue working with your existing Safend Data Protection Suite Clients.
Join a Cluster
Select this option if you already have at least one Management Server using an external database, and you would like to add another server to form a cluster.
< Back
Next >
Cancel

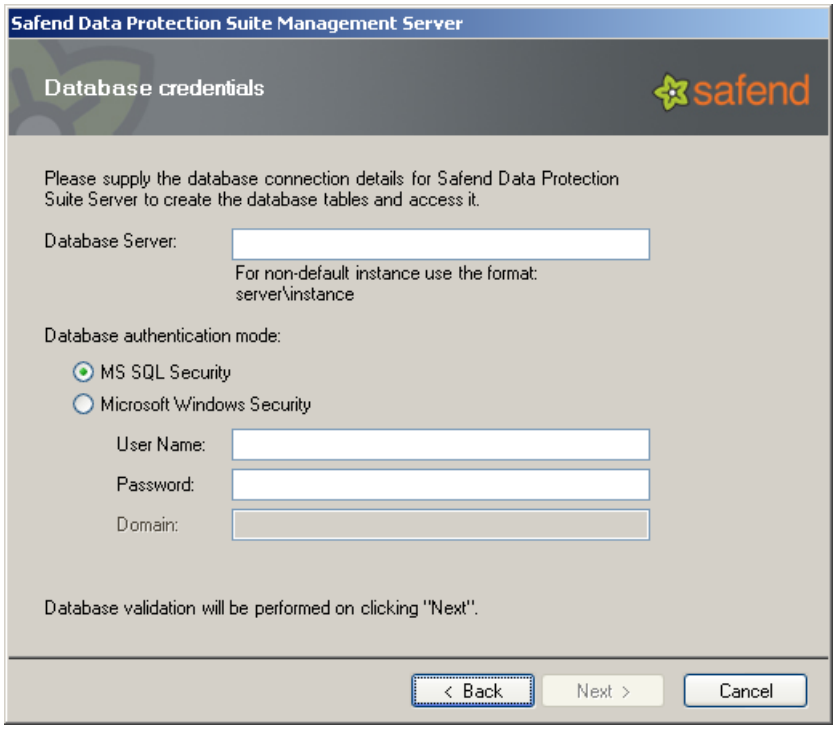
8. Select one of the following options:
   - For a new installation select the **New** radio button and proceed to step 9 below.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

- For instructions regarding the **Restore** option, refer to *Restoring an Existing Management Server* on page 28.
- To join a server cluster, select the **Join a Cluster** radio button.

  A server cluster enables the installation of several Safend Data Protection Suite Management Servers connected to a single external database, so that they seamlessly share the load of traffic from the endpoints, as well as provide redundancy and high availability.

  The following window opens:

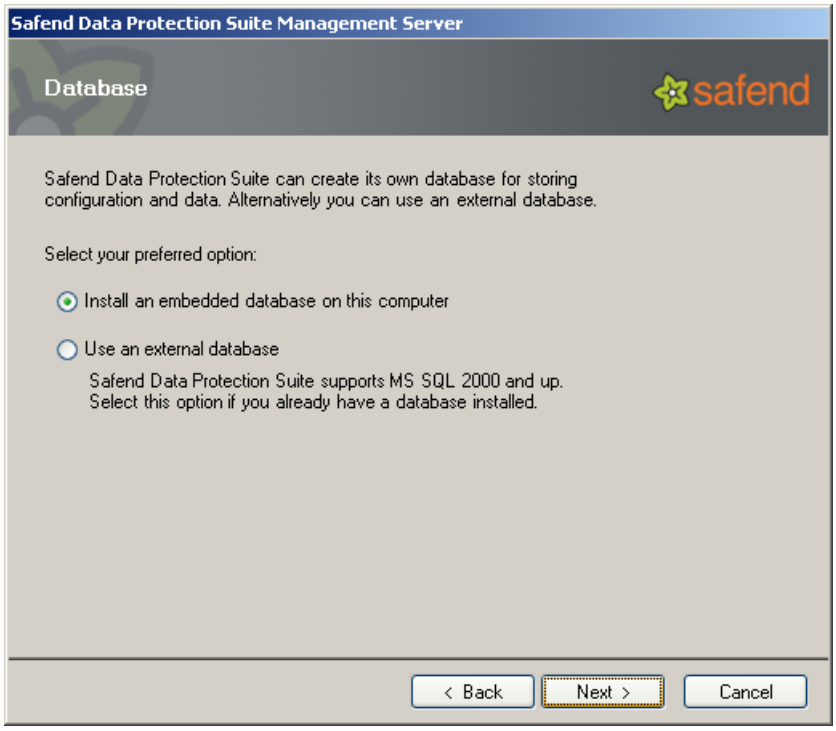

Safend Data Protection Suite Management Server
Database credentials
safend
Please supply the database connection details for Safend Data Protection Suite Server to create the database tables and access it.
Database Server:
For non-default instance use the format: server\instance
Database authentication mode:
MS SQL Security
Microsoft Windows Security
User Name:
Password:
Domain:
Database validation will be performed on clicking "Next".
< Back
Next >
Cancel

  Select the external database to which to connect.

  Proceed to step 12 below.

9. Click **Next**. The *Database* window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Safend Data Protection Suite Management Server
Database
safend
Safend Data Protection Suite can create its own database for storing configuration and data. Alternatively you can use an external database.
Select your preferred option:
Install an embedded database on this computer
Use an external database
Safend Data Protection Suite supports MS SQL 2000 and up.
Select this option if you already have a database installed.
< Back
Next >
Cancel

Safend Data Protection Suite can create its own internal database for storing configuration and data. Alternatively, you can use an existing external database.

NOTE

Safend Data Protection Suite supports MS SQL 2000 and above.

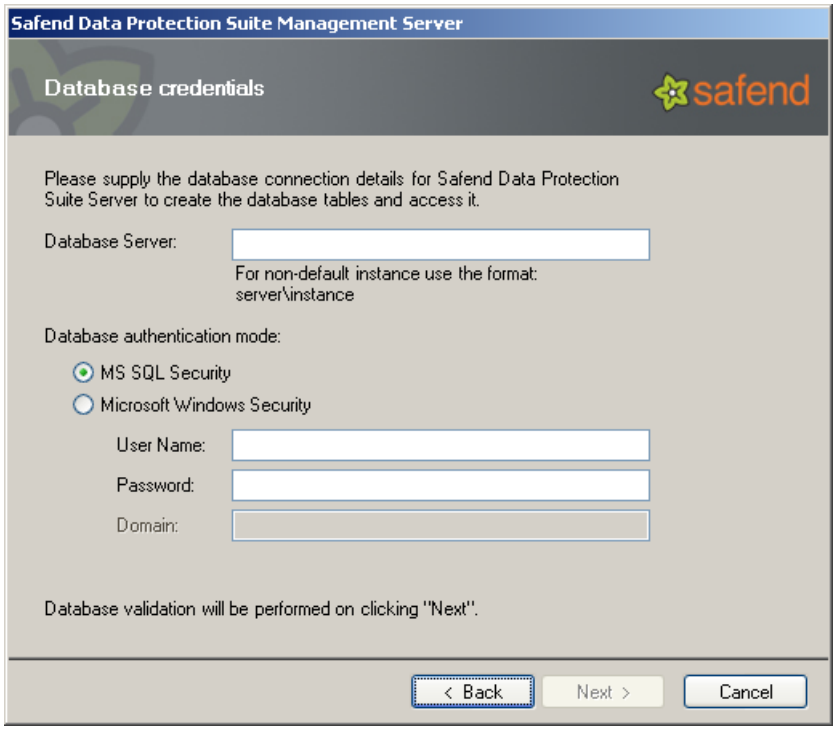
10. In the *Database* window, select the required radio button. Select the first radio button if you want to use a database which resides on the same machine as the Management Server (the database is managed by Safend Data Protection Suite Management Server). Select the second option if you have an MS SQL database on another machine and you want to use it as your Safend Data Protection Suite database.

NOTE

If you choose to use an existing external database, this database must already be installed.

11. Click **Next**. If you chose to install an embedded database, skip to *Step 15*.
12. If you have chosen to use an existing database server or to join a cluster, the following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Safend Data Protection Suite Management Server
Database credentials
safend
Please supply the database connection details for Safend Data Protection Suite Server to create the database tables and access it.
Database Server:
For non-default instance use the format: server\instance
Database authentication mode:
MS SQL Security
Microsoft Windows Security
User Name:
Password:
Domain:
Database validation will be performed on clicking "Next".
< Back
Next >
Cancel

13. In the *Database Credentials* window, perform the following steps:

    1. In the *Database Server* field, enter the database server name (for a non-default instance use the format `server\instance`).

    2. Under *Database authentication mode*, click the appropriate radio button to select whether to use **MS SQL Security** or **Microsoft Windows Security**.

    3. Enter the database authentication credentials – *User Name* and *Password*. If you selected **Microsoft Windows Security** you must also enter a *Domain* name.

14. Click **Next**. The installation program validates access to the database.

NOTE

If validation fails, re-enter the correct information, or click **Cancel** to exit the installation wizard.

NOTE

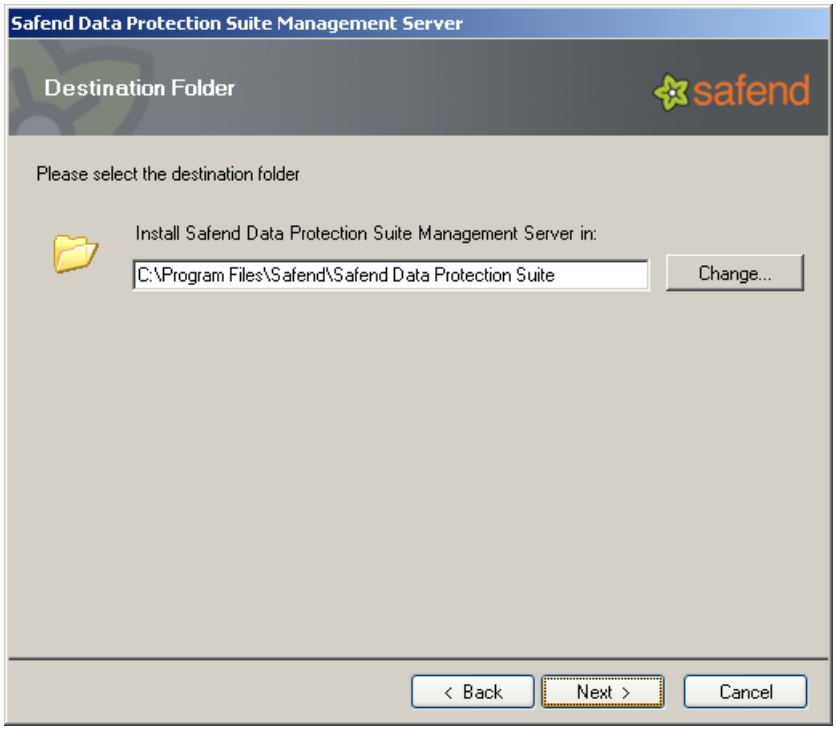
If a valid Safend Data Protection Suite database already exists on this database server, the following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Safend Protector Database Already Exists
According to your backup files a Safend Protector external database is, or was previously, used.
If you want to go on working with this database, go back and select "Connect to an existing database" option in the "Restore" windows of this wizard.
If you continue, and select to connect to your existing database, the information in it will be overwritten with the data in backup files.
Are you sure you want to continue?
Yes
No

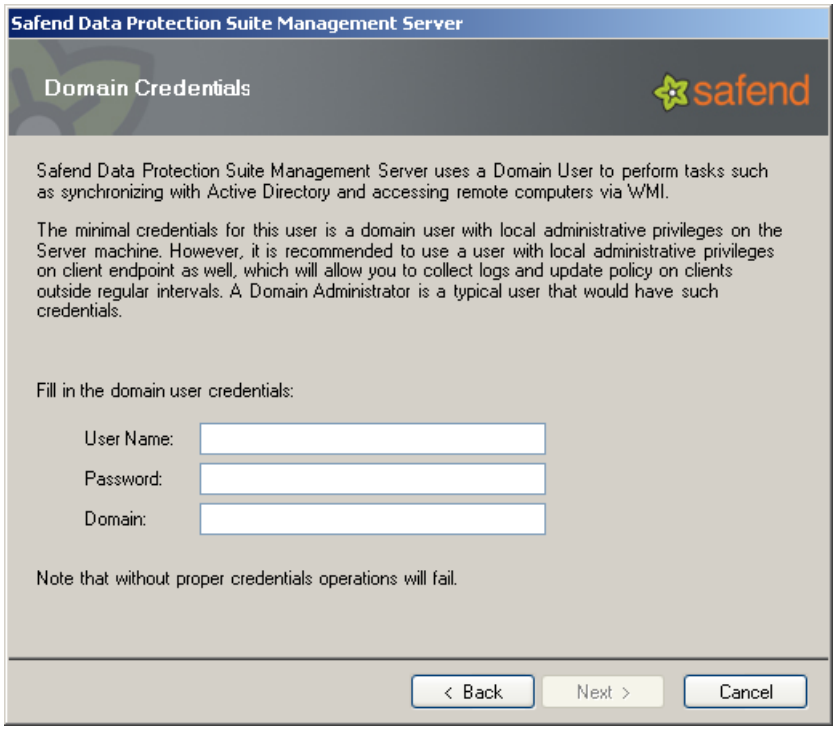
In this window, click **Yes** in order to overwrite the existing database. If you wish to use the existing database, click **No** and skip to *Restoring an Existing Management Server* on page 28.

15. The *Destination Folder* step opens:



16. Click **Next** to select the default installation folder: **`C:\Program Files\Safend\Safend Data Protection Suite`**, or click **Change** to select a different installation folder then click **Next**. The *Domain Credentials* window opens:

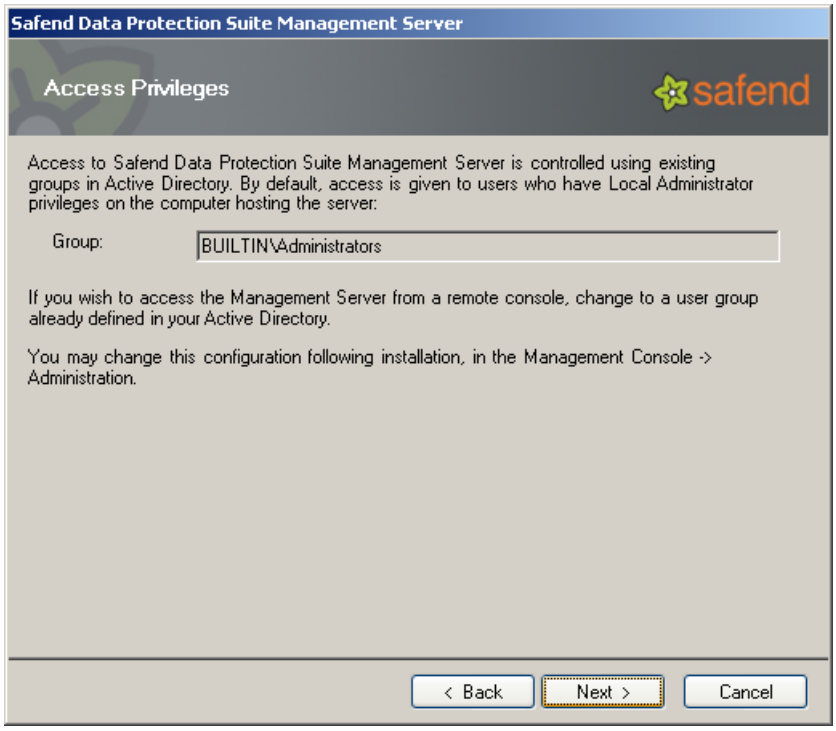
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Safend Data Protection Suite Management Server
Domain Credentials
safend
Safend Data Protection Suite Management Server uses a Domain User to perform tasks such as synchronizing with Active Directory and accessing remote computers via WMI.
The minimal credentials for this user is a domain user with local administrative privileges on the Server machine. However, it is recommended to use a user with local administrative privileges on client endpoint as well, which will allow you to collect logs and update policy on clients outside regular intervals. A Domain Administrator is a typical user that would have such credentials.
Fill in the domain user credentials:
User Name:
Password:
Domain:
Note that without proper credentials operations will fail.
< Back
Next >
Cancel

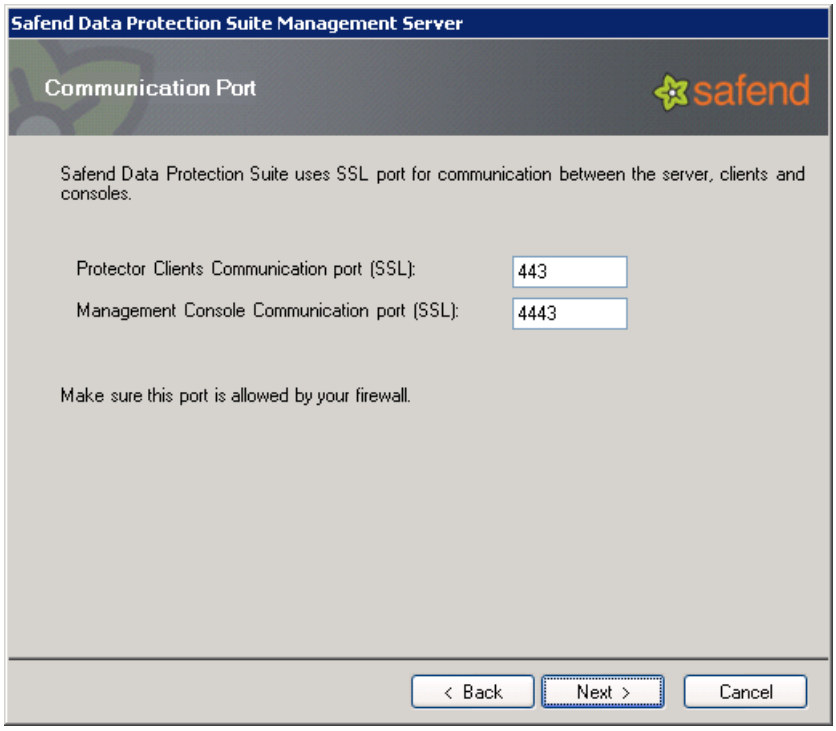
17. In the *Domain Credentials* window, enter the domain user credentials: Safend Data Protection Suite Management Server requires a domain account from your Active Directory in order to perform tasks such as creating GPOs and for controlling clients via WMI. We recommend that you enter an account with domain administrator privileges (you may change this user after installation).

18. Click **Next.**
    Users' access to the Management Console is restricted for security reasons. Safend Data Protection Suite does not require its own users and computers database. Instead, credentials are checked against Active Directory and/or local user accounts on the Management Server machine. Following installation, access to the Management Console is restricted to users who have local administrative rights on the computer hosting the Server, as shown below:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Safend Data Protection Suite Management Server
Access Privileges
safend
Access to Safend Data Protection Suite Management Server is controlled using existing groups in Active Directory. By default, access is given to users who have Local Administrator privileges on the computer hosting the server:
Group:
BUILTIN\Administrators
If you wish to access the Management Server from a remote console, change to a user group already defined in your Active Directory.
You may change this configuration following installation, in the Management Console -> Administration.
< Back
Next >
Cancel

19. Click **Next**. The *Communication Port* window opens.
    Safend Data Protection Suite Management Server communicates with the Safend Data Protection Suite Management Consoles and Clients through SSL ports. Safend Data Protection Suite uses two different ports to communicate with Safend Data Protection Suite Clients and with the Management Server.


Safend Data Protection Suite Management Server
Communication Port
safend
Safend Data Protection Suite uses SSL port for communication between the server, clients and consoles.
Protector Clients Communication port (SSL):
443
Management Console Communication port (SSL):
4443
Make sure this port is allowed by your firewall.
< Back
Next >
Cancel

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

The default ports are 443 for Clients communication and 4443 for Management Console communications. If you wish, you may change these default ports.

20. In order for SSL to operate, a certificate is needed to authenticate the Management Server. This certificate is also used for encrypting the data sent on the communication port. If the computer that is running the Server already has an active website that allows the SSL port activation, the application will use the existing certificate. If no certificate exists, the application will create a new certificate and will notify you of this.

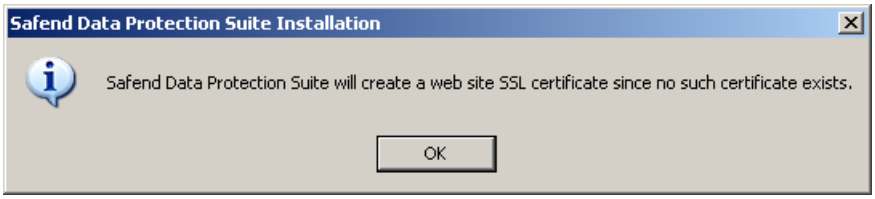
NOTE

A Safend generated certificate is not signed by a valid Certificate Authority (CA). Although this does not affect the overall security level of the system, using this certificate will cause Internet Explorer to display security alerts.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

In order to avoid these alerts you will need to replace the certificate with a signed certificate you receive from a trusted Certificate Authority.

21. Click **OK** to continue with the installation.

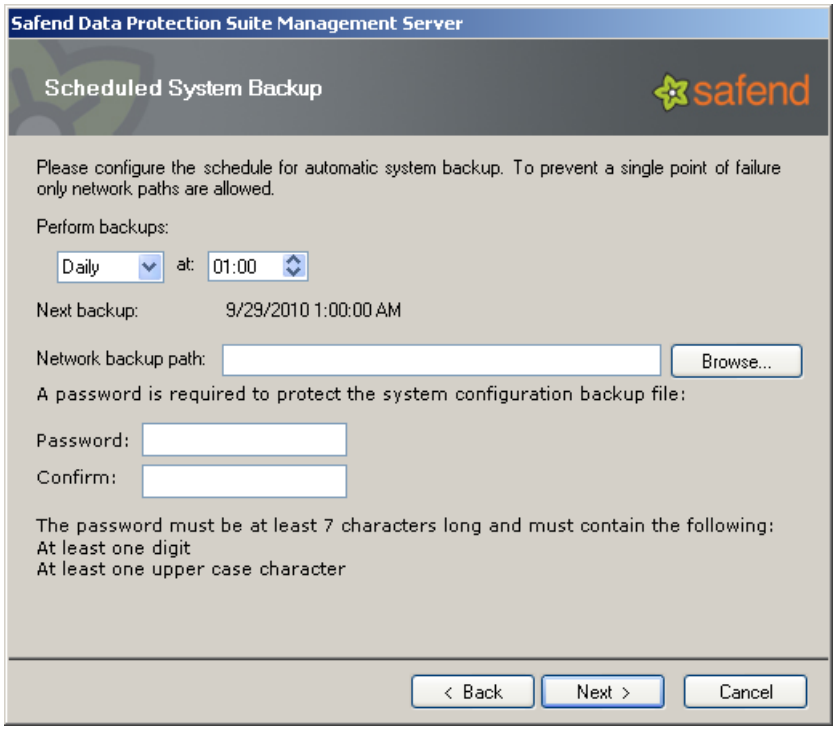

Safend Data Protection Suite Installation
Safend Data Protection Suite will create a web site SSL certificate since no such certificate exists.
OK

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

22. Click **Next**.
    In the following window, you will be asked to backup the system generated by Safend Data Protection Suite.

    To enhance the security of the system, encryption keys are generated during the installation. These keys are unique to your organization and raise the tampering resistance of your system. These keys are used to encrypt policies and logs as well as for mutual authentication between the Server and the endpoints. These keys as well as other information are protected when system backup is performed. For this reason it is highly recommended to backup the system on another machine/site in order to ensure smooth recovery in cases of server malfunction, without the need to re-deploy Clients to endpoints.

    In order to backup the system, you need to set a password that will be used to protect the system configuration backup file.


Safend Data Protection Suite Management Server
Scheduled System Backup
safend
Please configure the schedule for automatic system backup. To prevent a single point of failure only network paths are allowed.
Perform backups:
Daily
at:
01:00
Next backup:
9/29/2010 1:00:00 AM
Network backup path:
Browse...
A password is required to protect the system configuration backup file:
Password:
Confirm:
The password must be at least 7 characters long and must contain the following:
At least one digit
At least one upper case character
< Back
Next >
Cancel

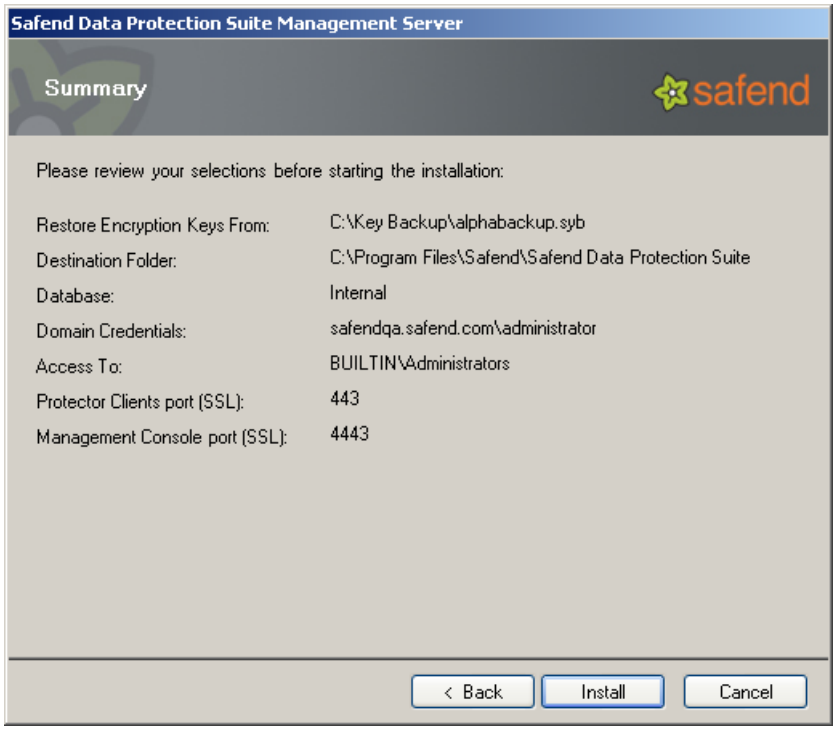
Select the day and time when automatic system backup will occur. To backup the system click **Browse** to select a path. Enter a *Password* and *Confirm* it.

NOTE

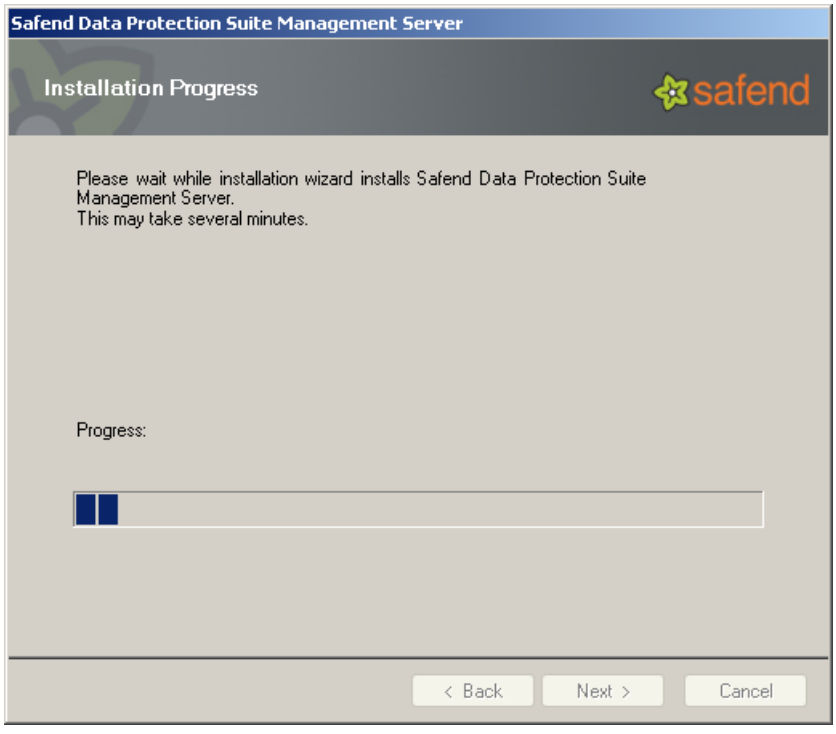
The password should be at least 7 characters long and should contain at least one digit and one upper case character.

23. Click **Next**. The *Summary* window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



24. Confirm the installation summary and click **Install** to install the Server. Installation begins and the *Installation Progress* window opens.


Safend Data Protection Suite Management Server
Installation Progress
safend
Please wait while installation wizard installs Safend Data Protection Suite Management Server.
This may take several minutes.
Progress:
< Back
Next >
Cancel

25. Once installation has been completed, the following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

26. The Safend Data Protection Suite Management Server has been installed. Check *Launch Management Console* at the bottom of the screen if you wish to launch the Safend Data Protection Suite Management Console, and click **Finish**.

NOTE

The installation process installs the Safend Data Protection Suite Management Console as well.

27. If you've chosen to launch the Safend Data Protection Suite Management Console, the *Login* window opens.

Enter your *User Name*, *Password* and *Domain* and click **Login**. The application opens, displaying the main window.

28. Take the time to define preliminary settings in the *Administration* and *Global Policy Settings* windows. Please refer to the *Post-Installation Settings (Checklist)* on page 37 for a list of settings which you may want to review and change.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Restoring an Existing Management Server

NOTE

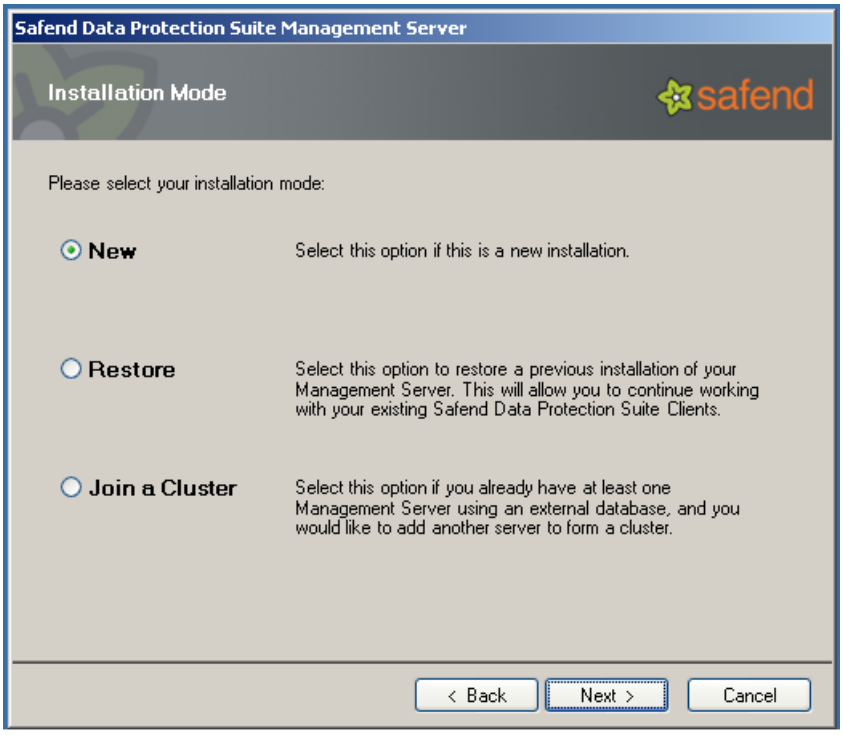
If you have an encrypted machine, you cannot install a new server and connect it to the clients. You must first backup and then perform restore.

In some cases you will need to install Safend Data Protection Suite Management Server while maintaining your system's unique encryption keys, in order to work with your existing Safend Data Protection Suite Clients. This may happen when you want to migrate the Server from a low-CPU machine to a more powerful one, or when recovering from hardware malfunctions.

In order to restore an existing Management Server you will need to provide the encryption keys backup file and the password that was set to protect it.

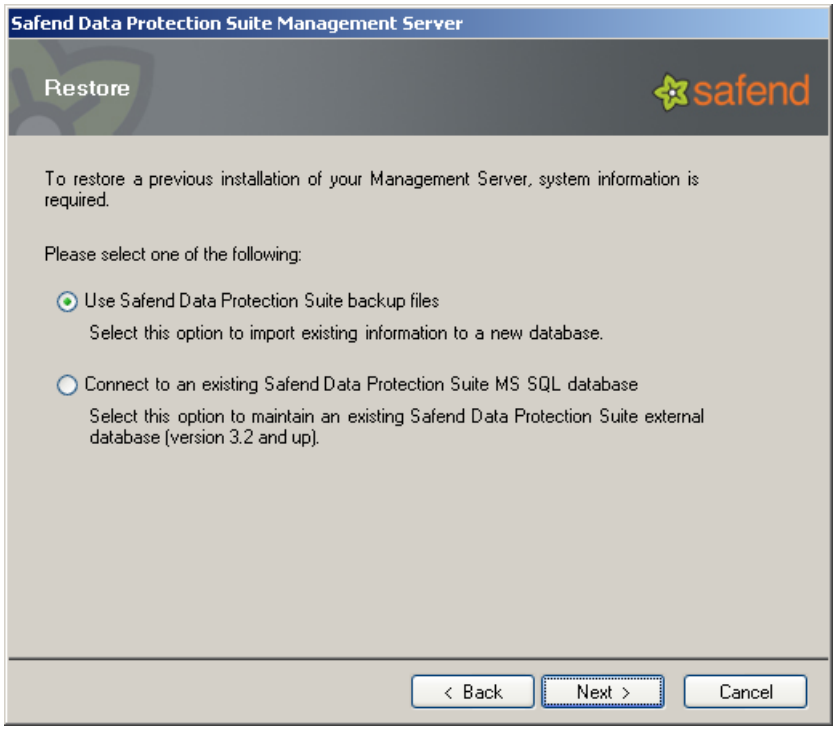
➢ To restore an existing Management Server:

1. Perform the steps described in *Installing the Management Server* on page 15 up to Step 7.
2. At this stage, you will be asked to choose the installation mode, as shown below:


Safend Data Protection Suite Management Server
Installation Mode
safend
Please select your installation mode:
New
Select this option if this is a new installation.
Restore
Select this option to restore a previous installation of your Management Server. This will allow you to continue working with your existing Safend Data Protection Suite Clients.
Join a Cluster
Select this option if you already have at least one Management Server using an external database, and you would like to add another server to form a cluster.
< Back
Next >
Cancel

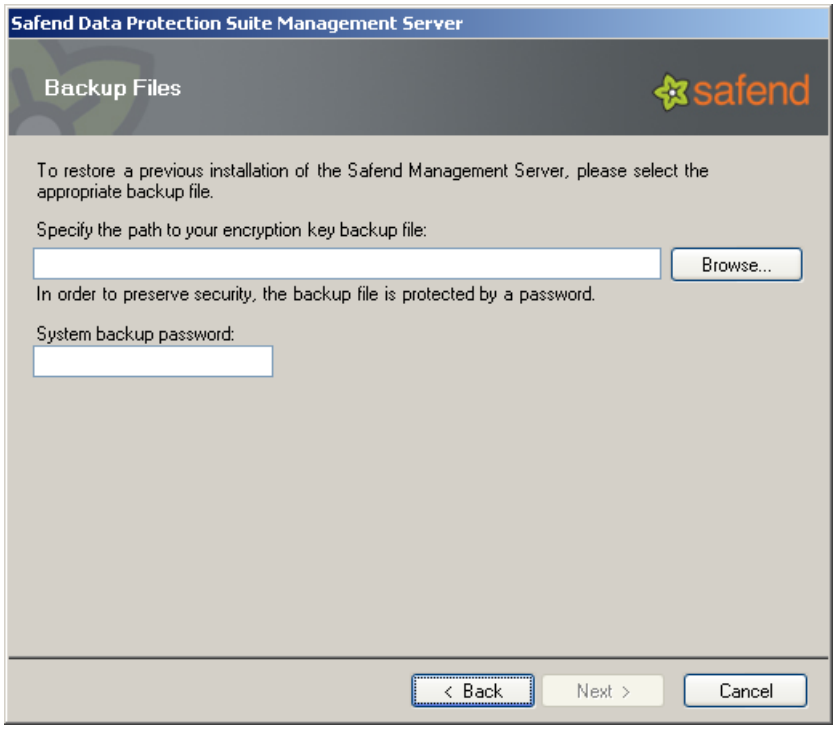
3. Select the **Restore** radio button. The following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Safend Data Protection Suite Management Server
Restore
safend
To restore a previous installation of your Management Server, system information is required.
Please select one of the following:
Use Safend Data Protection Suite backup files
Select this option to import existing information to a new database.
Connect to an existing Safend Data Protection Suite MS SQL database
Select this option to maintain an existing Safend Data Protection Suite external database (version 3.2 and up).
< Back
Next >
Cancel

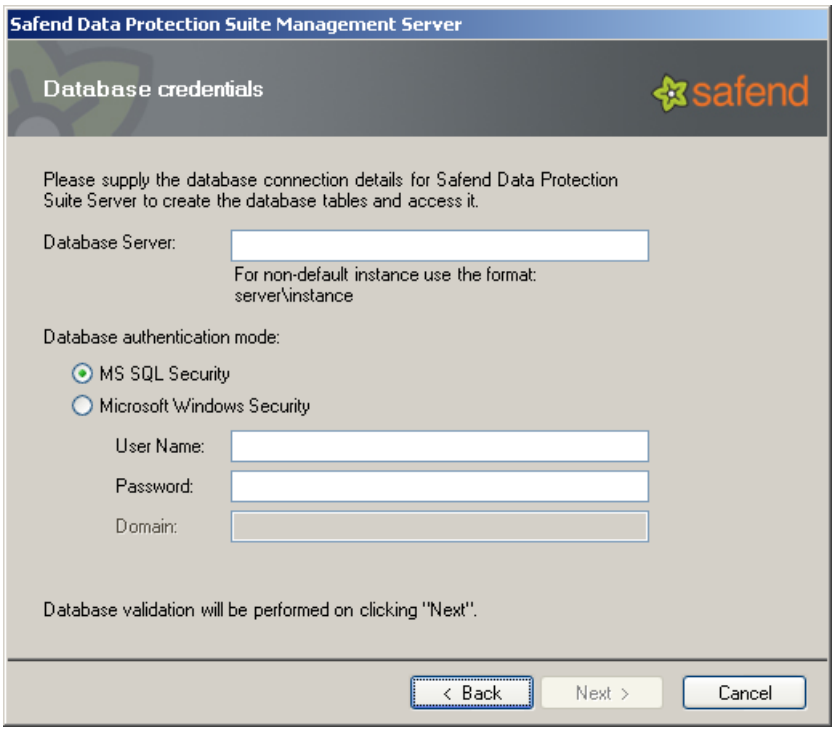
4. In the *Restore* window, select the appropriate radio button according to whether you wish to use Safend Data Protection Suite backup files or connect to an existing external Safend Data Protection Suite MS SQL database. If you select the second option, *Connect to an existing Safend Data Protection Suite MS SQL database*, skip to *step 8* below.

5. Click **Next**. The *Backup Files* window opens:


Safend Data Protection Suite Management Server
Backup Files
safend
To restore a previous installation of the Safend Management Server, please select the appropriate backup file.
Specify the path to your encryption key backup file:
Browse...
In order to preserve security, the backup file is protected by a password.
System backup password:
< Back
Next >
Cancel

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

6. Enter the path to your keys backup file and the password protecting it.
7. Skip to *step 11* below.
8. If you have chosen to use an existing database server, the following window opens:


Safend Data Protection Suite Management Server
Database credentials
safend
Please supply the database connection details for Safend Data Protection Suite Server to create the database tables and access it.
Database Server:
For non-default instance use the format: server\instance
Database authentication mode:
MS SQL Security
Microsoft Windows Security
User Name:
Password:
Domain:
Database validation will be performed on clicking "Next".
< Back
Next >
Cancel

9. In the *Database credentials* window, perform the following steps:

    1. In the *Database Server* field, enter the database server name (for a non-default instance use the format `server\instance`).

    2. Under *Database authentication mode*, click the appropriate radio button to select whether to use **MS SQL Security** or **Microsoft Windows Security**.

    3. Enter the database authentication credentials – *User Name* and *Password*. If you selected **Microsoft Windows Security** you must also enter a *Domain* name.

10. Click **Next**. The installation program validates access to the database.

NOTE

If validation fails, re-enter the correct information, or click **Cancel** to exit the installation wizard.

11. Follow the instructions in steps 15-26 in *Installing the Management Server*.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Upgrading the Management Server

From time to time it may be necessary to upgrade the Safend Data Protection Suite Management Server. There is a wizard which enables you to easily upgrade the Management Server on your computer.
The Safend Upgrade Procedure is performed in two steps. In the first step, the server is upgraded to the new version, while the agents installed on the endpoints in the organization are still of the older version. The old agents are fully managed by the new server. In the second step, the existing agents are upgraded to the new version using the agent installation files created by the new server.

Considerations Before Performing Management Server Upgrade

- In this version, upgrade and backward computability are supported from Safend Data Protection Suite 3.3 SP7 and up. If you are currently using an older version of Safend Data Protection Suite, or have legacy agents in your environment which were not upgraded yet, it is recommended that you don't perform an upgrade using this version of the Safend Data Protection Suite.
- The system upgrade will maintain all policies and definitions after the upgrade process. However, existing (history) log records will no longer be available. Customers are advised to backup the DB prior to the upgrade if log data is needed to be kept for future use. Restore of the backed up DB should be done to a separate server in a separate environment if needed.
- There are several features which were supported in Safend Data Protection Suite 3.3 and are no longer supported in Safend Data Protection Suite version 3.4. Before performing an upgrade, please make sure you are not using these features. These features are specified in a separate document: *Safend Data Protection Suite v3.4 – Upgrade Instructions*, available from Safend.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

- When upgrading the Management Server to version 3.4, all your existing policies will undergo an upgrade procedure. In Safend Data Protection Suite version 3.4, instead of having one policy which defines all aspects of the endpoint behaviour, you will now have separate policies managing separate aspects of the endpoint behaviour. Port control, device control and removable media encryption will be controlled using a Port & Device Control Policy; encryption of the internal hard disk will be enforced using a Hard Disk Encryption policy; endpoint configuration, such as the log sending interval, will be controlled using the Settings Policy. For additional information, refer to *Safend Data Protection Suite v3.4 – Upgrade Instructions*, available from Safend.

  Recommended action: to avoid the creation of multiple, redundant policies following the server upgrade, please review your existing policies to make sure policies are not configured to use "policy specific settings" instead of "global policy settings" without a good reason. From our experience, most customers do not need to configure different settings for different machines in the organization using "Policy Specific Settings", and can use a consistent configuration throughout the organization using "Global Policy Settings". After upgrade, again review all policies and remove multiple or redundant policies.
- Before performing the upgrade, it is highly recommended to create an updated System Backup file (created through the Administration -> Maintenance tab). This file will be used to restore the existing server in case the upgrade procedure is not completed successfully.
- After the Server Upgrade, you should review the Hard Disk Encryption Policies. In case you are using Safend Encryptor to encrypt machines in your organization, some Hard Disk Encryption policies will be created following the server upgrade. Your organization should have at any point in time no more than two Hard Disk Encryption Policies: an "Encrypt" policy which enforces the encryption on the appropriate workstations in your environment, and (optionally) a "Decrypt" policy excluding specific workstations from the general encryption policy. Remember, Hard Disk Encryption policies only apply on machines, not on users. There is no reason to associate a Hard Disk Encryption policy to a user object, or to another object (Group or OU) which only contains user objects.

➢ To upgrade the Management Server:

NOTE

Before Upgrading the Management Server you must remove Safend Data Protection Suite Console and all remote consoles as described in *Uninstalling Safend Data Protection Suite Management Console* on page 48. After completing server upgrade, you must again reinstall the consoles, as described in *Installing Safend Data Protection Suite Management Console* on page 41.

1. Locate *SafendDataProtectionSuite.exe* on your installation CD.
2. Double-click the file. The *Safend Data Protection Suite Management Server* installation window is displayed.
3. Click **Browse** to select a destination folder for the extracted installation files.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

NOTE

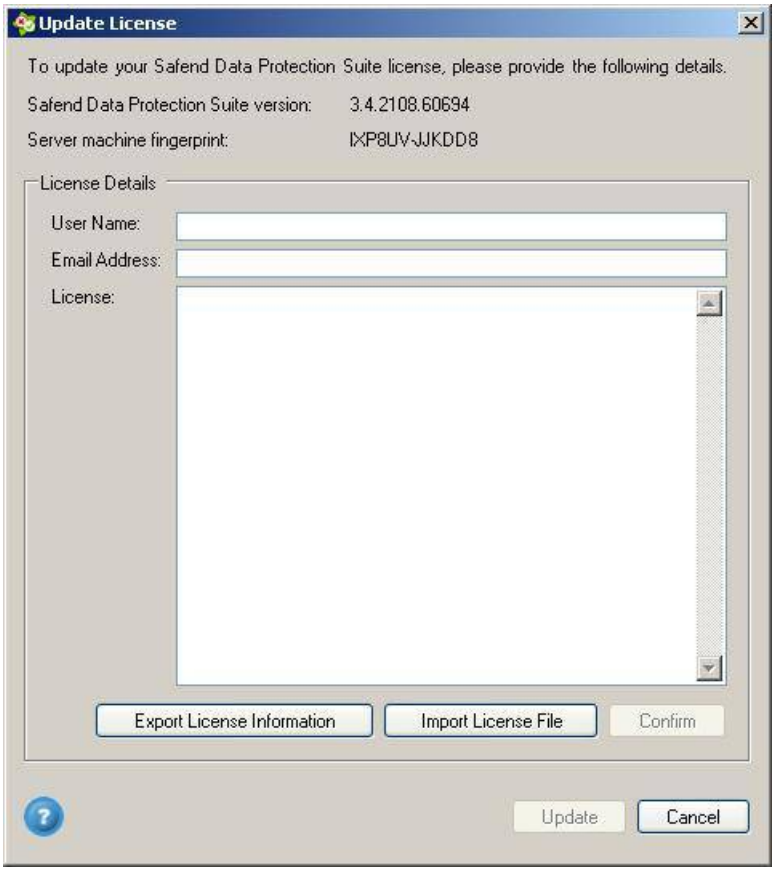
Make sure that the files are extracted to a local folder. The installation will not run from a network path.

4. Click **Install**.
5. Following extraction, you will be asked to select the Safend Data Protection Suite Server language.
6. Select the required language and click **OK**. The first step of the Safend Management Server Upgrade wizard is displayed.

Safend Data Protection Suite Management Server
SAFEND
Management Server
Upgrade
This wizard will upgrade Safend Data Protection Suite Management Server on your computer.
Note: it is highly recommended to manually backup your logs before upgrading, as these will be lost if the upgrade fails. Other data is automatically backed up and will not be lost.
Warning: This program is protected by copyright law and international treaties.
safend
Click Next to continue with the upgrade or Cancel to exit.
< Back
Next >
Cancel

7. Click **Next**.
8. In the following window provide your license update information.

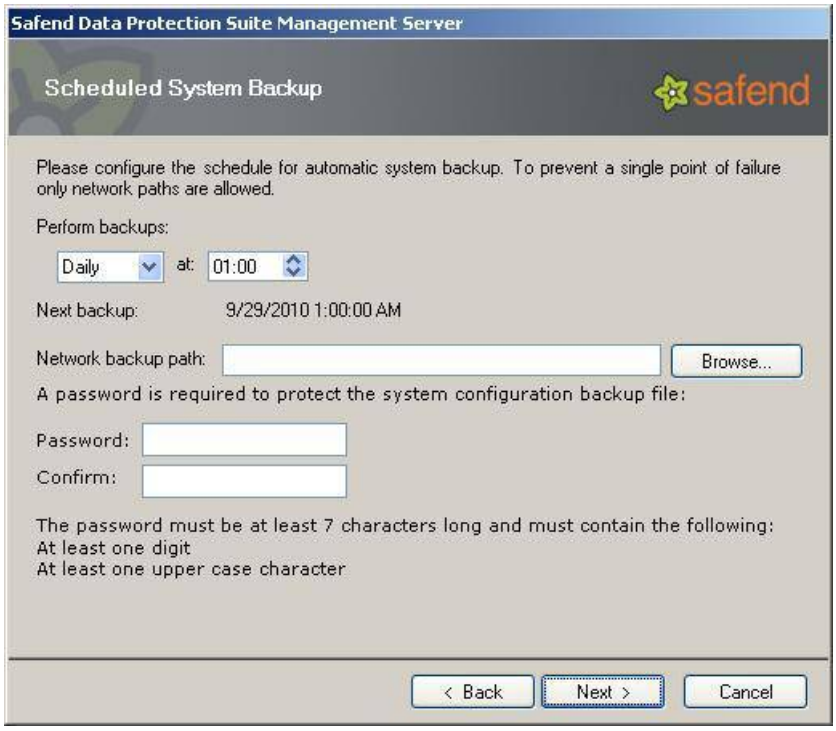
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



Enter your **User Name** and **Email Address**. In order to obtain a license key, contact Safend or your local reseller and provide the Server machine fingerprint as it appears in the screen. For example, the fingerprint in the window above is: IXP8UV-JJKDD8. Using this fingerprint, a license key will be generated for you and can only be used on this specific machine. You also have the option to export license information or to import a license file. Click **Update**.

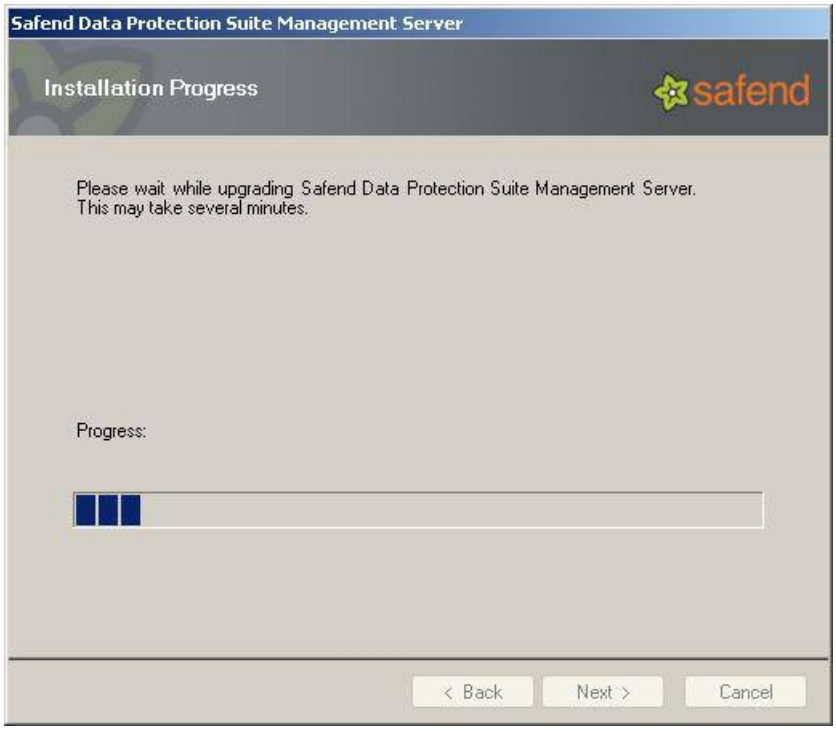
9. You will now be asked to enter information in order to perform automatic system backup.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Safend Data Protection Suite Management Server
Scheduled System Backup
safend
Please configure the schedule for automatic system backup. To prevent a single point of failure only network paths are allowed.
Perform backups:
Daily
at:
01:00
Next backup:
9/29/2010 1:00:00 AM
Network backup path:
Browse...
A password is required to protect the system configuration backup file:
Password:
Confirm:
The password must be at least 7 characters long and must contain the following:
At least one digit
At least one upper case character
< Back
Next >
Cancel

Enter the day and time. Click **Browse** to select a network backup path. Enter a password and confirm it. Click **Next** after entering the information.

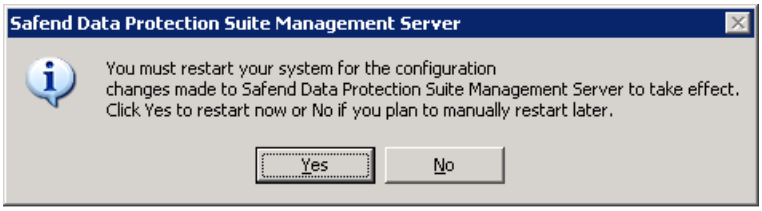
10. The Installation Progress window will now be displayed.



11. The following screen will be displayed when the process is completed. Click **Finish**.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

12. You will now be asked to restart your system. It is highly recommended that you restart your system in order for the changes to take effect.


Safend Data Protection Suite Management Server
You must restart your system for the configuration changes made to Safend Data Protection Suite Management Server to take effect.
Click Yes to restart now or No if you plan to manually restart later.
Yes
No

Upgrading a Clustered Server Environment

Here is the procedure to follow when upgrading a clustered server environment.

➢ To upgrade a Server Cluster:

1. Uninstall cluster nodes and leave one primary server active. We recommend leaving the server that has the most resources out of all the nodes in the cluster.
2. Upgrade the primary server that was left active to the latest Safend Data Protection server version.
3. Install additional cluster nodes using the latest Safend Data Protection Server version. This can be achieved by selecting the *Join a Cluster* option from the Safend Data Protection Suite Management Server installation wizard.
4. Upgrade the Safend Data Protection clients as described in Chapter 5 on page 49.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Post-Installation Settings (Checklist)

The Safend Data Protection Suite Management Server installation package defines default settings for system behavior which you can find under **Administration** and **Global Policy Settings** (both available from the *Tools* menu in the *Safend Data Protection Suite Management Console*).
Once you complete installing Safend Data Protection Suite Management Server and access the Management Console, you may want to access these windows and set the parameters relevant to your environment.

Checklist for the Most Critical Settings in the Administration Window

1. **Encryption Keys Backup -** If you have not backed up the encryption keys during installation**.**
2. **Client Installation Folder** - Set a shared folder for creating client installation files. You will need these files in order to install clients.

Refer to *Chapter 12, Administration* in the *Safend Data Protection Suite User Guide* for an explanation of Administration settings.

Checklist for the Most Critical Settings in the Global Policy Settings Window

1. **Log Transfer Interval** – Define the frequency in which logs will be sent from endpoints to the Server.

IMPORTANT

Be especially careful when configuring the *Logs Transfer Interval,* in order not to burden your network and endpoints with excessive log sending.

Consider the following:

- The number of endpoints in your network.
- The number of expected events from each endpoint (client and file logs).
- The level of need for "real time" log information in the Management Console.

During installation, the default log interval is set to 90 minutes. In the case of large scale deployments, please consult Safend Support in order to optimize your settings.

2. **Clients Uninstall Password** – Change the default password to your own preference.

IMPORTANT

Upon product installation the password is set to "**Password1**". Since the password is one of the foundations for the tamper resistance of the client, it is highly recommended that you change it as soon as you start deploying the product in a production environment.

IMPORTANT

Make sure you have created a backup for the Server encryption keys. This will prevent situations in which you cannot uninstall Clients due to password loss.

Refer to *Chapter 7, Configuring Policies* in the *Safend Data Protection Suite User Guide* for an explanation about the Global Policy settings.

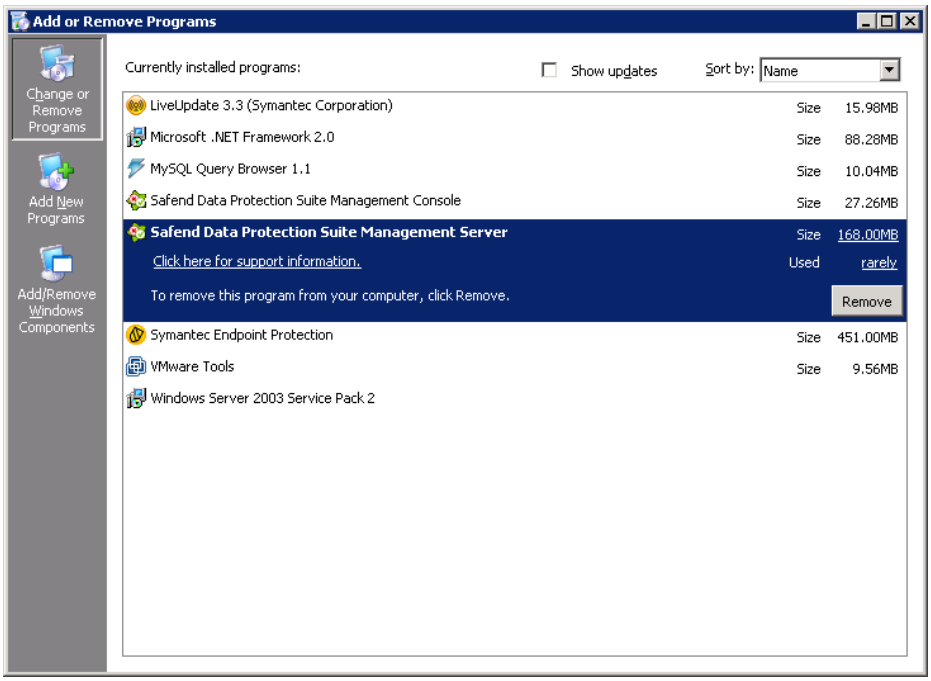
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Uninstalling Safend Data Protection Suite Management Server

Here is the procedure for uninstalling the Management Server.

➢ To uninstall the Management Server:

1. Open **Add or Remove Programs** from Control Panel.
2. Select the Safend Data Protection Suite Management Server from the list, and click **Remove** as shown here:



NOTE

Uninstalling Safend Data Protection Suite Management Server will delete the Safend Data Protection Suite database; therefore, if you wish to install the latest Server version, it is recommended to upgrade your Server rather than to perform an uninstall/install process.

Changing your Database

If you wish to change from using a Safend Data Protection Suite embedded database to an external MS SQL database, or vice versa, you can do so by using the Restore option as explained in *Restoring an Existing Management Server* on page *28* and selecting the new database type.

NOTE

You can only change your database if you are using version 3.2 and above.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

IMPORTANT

Changing your database will result in a loss of previous logs. Previous policies are transferred to the new database, but policy associations with organizational objects (when using the "direct distribution from the Management Server to Clients" policy distribution mode) are lost.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Chapter 4

Installing Safend Data Protection Suite Management Console

About This Chapter

This chapter describes how to install the Safend Data Protection Suite Management Console. It contains the following sections:

- ✓ ***Prerequisites***, page 41, describes the prerequisites of the Management Console.
- ✓ ***Installing Prerequisite Software***, page 41, describes how to install Microsoft .NET framework.
- ✓ ***Installing Safend Data Protection Suite Management Console***, page 41, describes two methods for installing the Console.
- ✓ ***Launching Safend Data Protection Suite Management Console for the First Time***, page 47, describes how to launch Safend Data Protection Suite Management Console.
- ✓ ***Uninstalling Safend Data Protection Suite Management Console***, Page 48, describes how to uninstall Safend Data Protection Suite Management Console.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Prerequisites

NOTE

Refer to the *What's New* document for the most up-to-date system requirements.

Installing Prerequisite Software

Installing Microsoft .NET Framework 2.0

➢ To install .NET Framework

Refer to *Installing Prerequisite Software* on page 13.

Installing Safend Data Protection Suite Management Console

Safend Data Protection Suite Management Console can be installed and run from any computer on your network. The first console is installed on the same machine that hosts the Management Server as part of the Server installation, and additional consoles can be installed on any machine in your domain that meets the prerequisites.

Additional consoles can be installed on your domain either through Safend's Management Console Installation web page (recommended), or by running the ManagementConsole.msi file from an external source, such as a CD.

NOTE

Access to the Management Consoles is restricted by default to the local administrators group of the machine hosting the server. In order not to expose your server machine user and password unnecessarily, make sure you change this setting to a user group in your Active Directory before installing additional Management Consoles. You can change this setting from the Administration window in the Management Console.

Installing the Console from the Installation Web Page

Safend Data Protection Suite Management console features a '*One-click*' deployment process which gives you easy access to installing the Management Console by pointing your browser to the Safend Management Server address. This method automatically keeps all your Management Consoles up-to-date with the latest software version of the Management Server, and is therefore the recommended installation method.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

➢ To install the Management Console from the installation web page:

1. Access the address of the installation web page in the target machine.
   The link is in the following format:

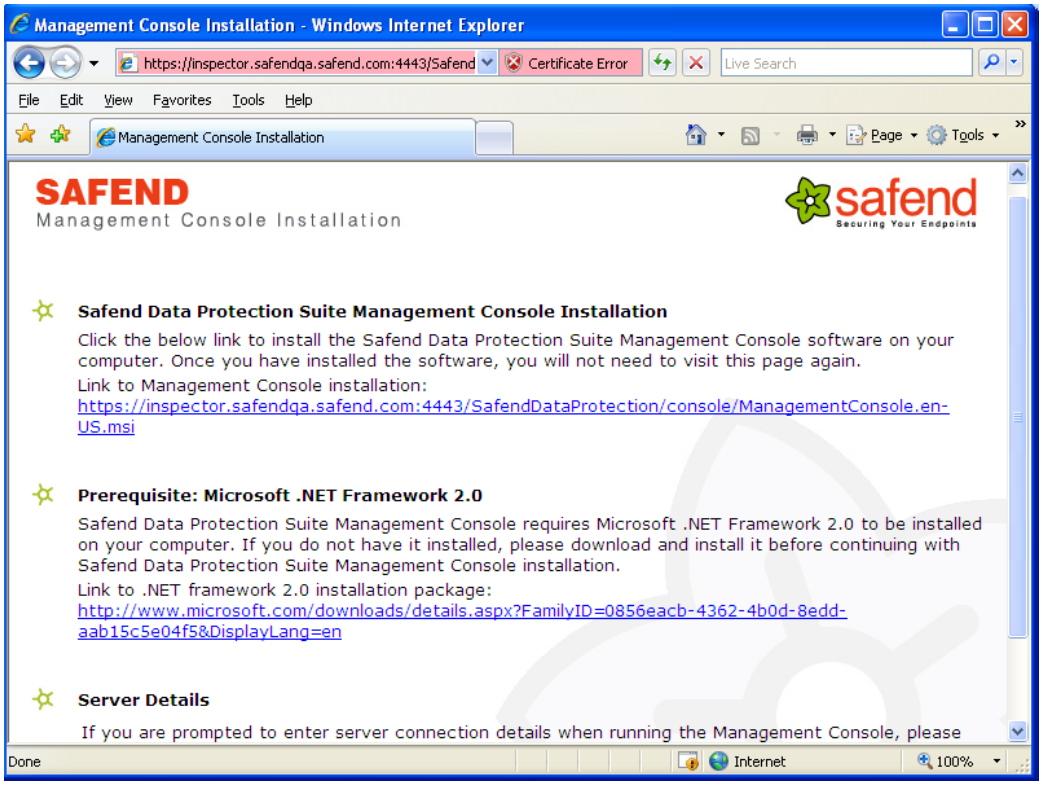
https://<servername>:<serverport>/SafendDataProtection/consoleinstall.aspx

TIP

You may also use a shorter link format:
https://<servername>:<serverport>/SafendDataProtection

This address can be found in the *General* tab of the *Administration* window, which you can access from the Management Console's *Tools* menu.

The installation page opens:

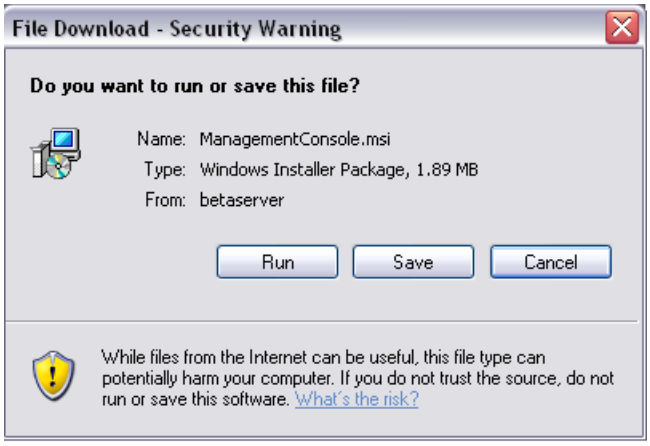

Management Console Installation - Windows Internet Explorer
https://inspector.safendqa.safend.com:4443/Safend
Certificate Error
Live Search
File Edit View Favorites Tools Help
Management Console Installation
Page Tools
SAFEND
Management Console Installation
safend
Securing Your Endpoints
Safend Data Protection Suite Management Console Installation
Click the below link to install the Safend Data Protection Suite Management Console software on your computer. Once you have installed the software, you will not need to visit this page again.
Link to Management Console installation:
https://inspector.safendqa.safend.com:4443/SafendDataProtection/console/ManagementConsole.en-US.msi
Prerequisite: Microsoft .NET Framework 2.0
Safend Data Protection Suite Management Console requires Microsoft .NET Framework 2.0 to be installed on your computer. If you do not have it installed, please download and install it before continuing with Safend Data Protection Suite Management Console installation.
Link to .NET framework 2.0 installation package:
http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en
Server Details
If you are prompted to enter server connection details when running the Management Console, please
Done
Internet
100%

This page contains the following:

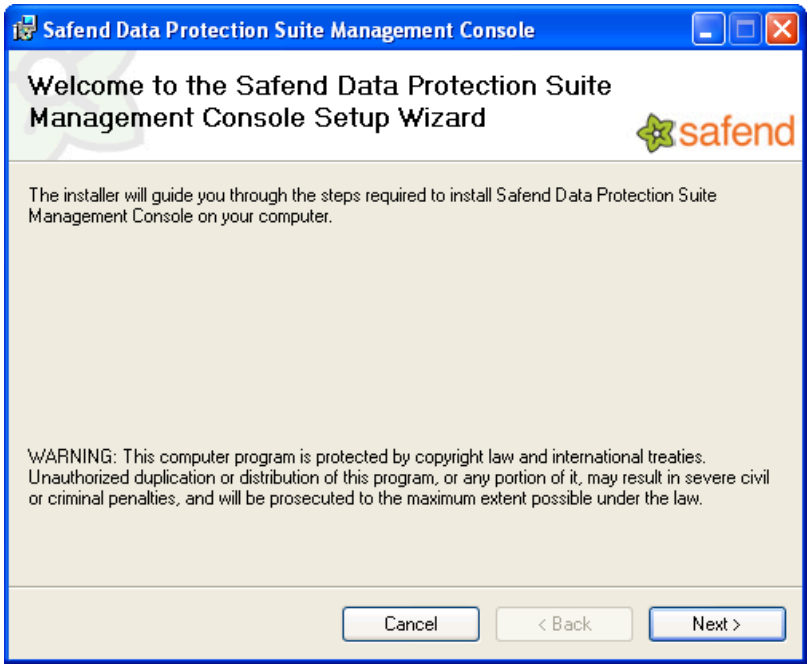
- A link to the Microsoft .NET framework 2.0 installation package.
- A link to the Management Console installation package.
- Server details.

2. If the machine on which you wish to install an additional Console does not have .NET framework installed, enter the link and install it before proceeding with the Management Console installation.
3. Click the link to the Management Console installation package. The following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

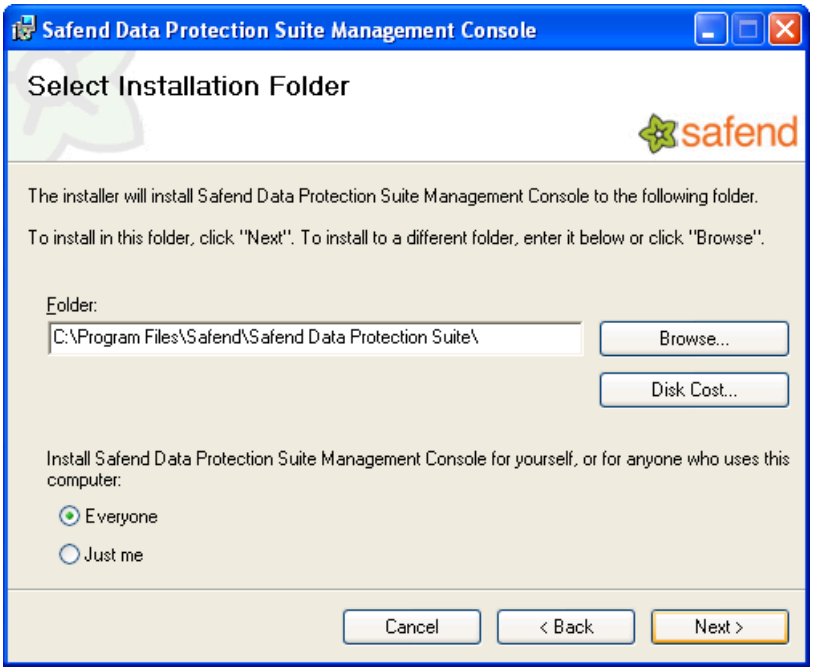

File Download - Security Warning
Do you want to run or save this file?
Name: ManagementConsole.msi
Type: Windows Installer Package, 1.89 MB
From: betaserver
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

4. Click **Run**. The Management Console installation wizard opens:


Safend Data Protection Suite Management Console
Welcome to the Safend Data Protection Suite Management Console Setup Wizard
safend
The installer will guide you through the steps required to install Safend Data Protection Suite Management Console on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

5. Click **Next.** The *Select Installation Folder* window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

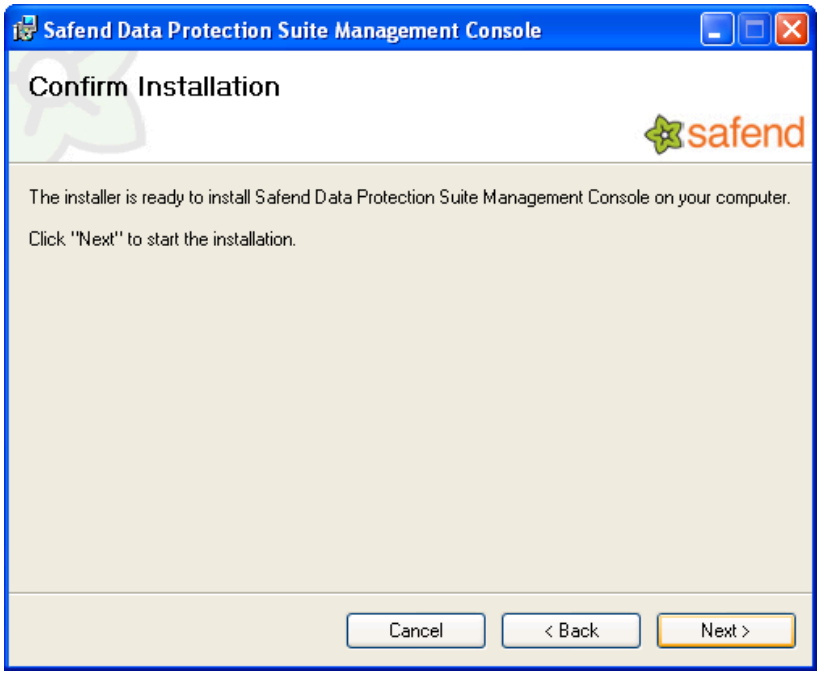

Safend Data Protection Suite Management Console
Select Installation Folder
safend
The installer will install Safend Data Protection Suite Management Console to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files\Safend\Safend Data Protection Suite\
Browse...
Disk Cost...
Install Safend Data Protection Suite Management Console for yourself, or for anyone who uses this computer:
Everyone
Just me
Cancel
< Back
Next >

6. In the *Select Installation Folder* window, select the folder in which the Safend Data Protection Suite Management console will be installed. The default folder is C:\Program Files\Safend\Safend Data Protection Suite\. If you wish to install the Management Console in a different folder, click the **Browse** button and select the desired folder.

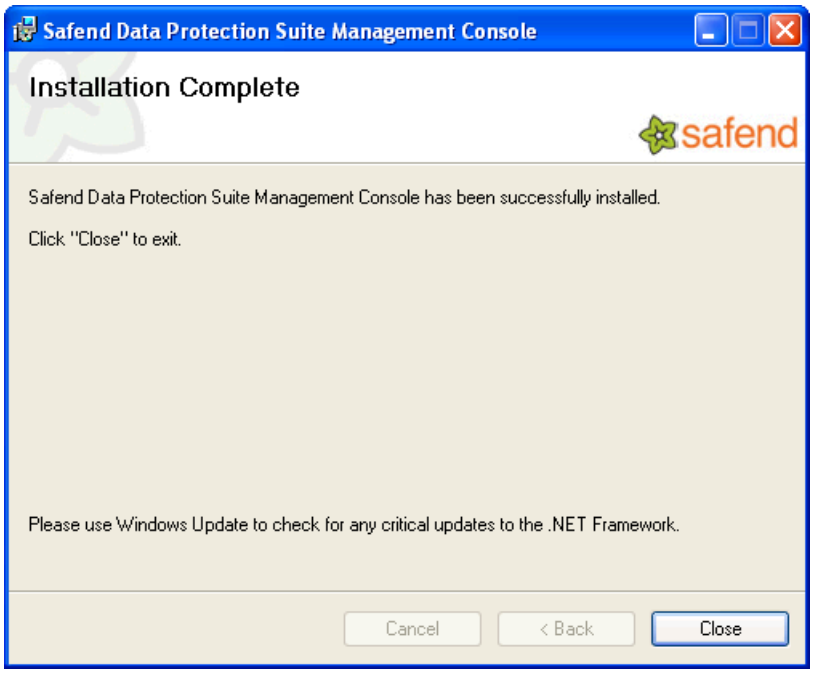
7. Select one of the following options by clicking its radio button:
   - **Everyone**: allows access to the application to all users who use the computer.
   - **Just me**: allows access to the application to the logged on user only.

8. Click **Next**. The following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

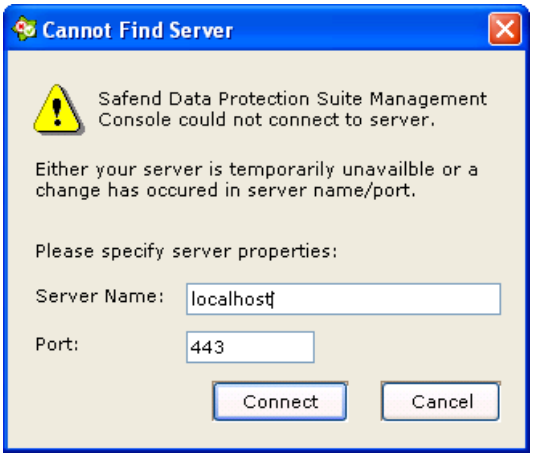

Safend Data Protection Suite Management Console
Confirm Installation
safend
The installer is ready to install Safend Data Protection Suite Management Console on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next >

9. In the *Confirm Installation* window, click **Next** to perform the installation.
10. Once the installation completes, the following window opens:


Safend Data Protection Suite Management Console
Installation Complete
safend
Safend Data Protection Suite Management Console has been successfully installed.
Click "Close" to exit.
Please use Windows Update to check for any critical updates to the .NET Framework.
Cancel
< Back
Close

11. Click **Close** to exit.
12. Open the Management Console application by clicking the icon on your desktop or from **Start > Programs > Safend Data Protection Suite > Management Console**.
13. Depending on the browser you are using, the following message may appear:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



Fill in the *Server Name* and *Port* as it appears in the installation web page, and click **Connect**.

14. The *Login* window appears:

Type your *User Name*, *Password* and *Domain* and click **Login**. The application will open, displaying the main window.

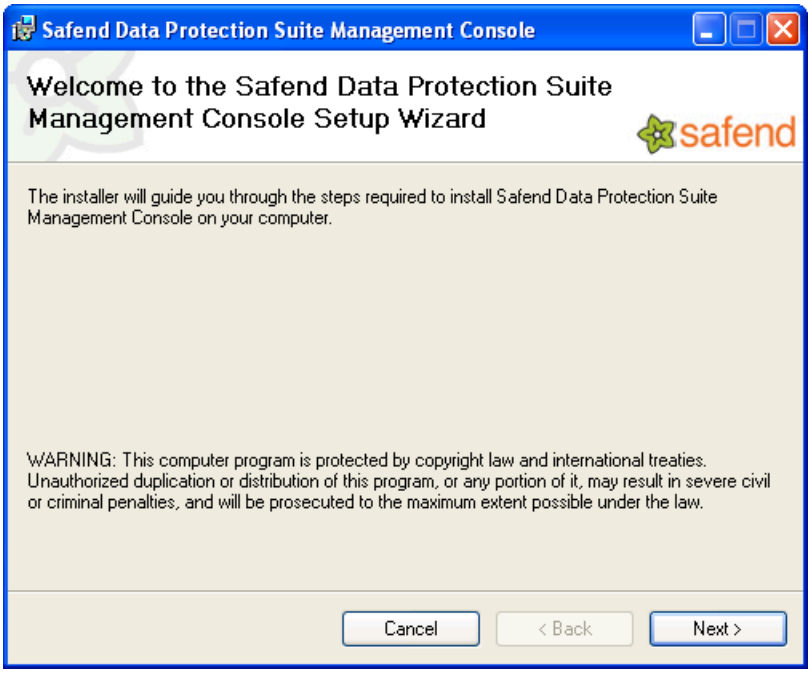
Installing Safend Data Protection Suite Management Console Manually

Here is a descripton of how to manually install the console.

➢ To manually install the Management Console:

1. Locate the *ManagementConsole.msi* file on your CD and run it. The setup window opens:

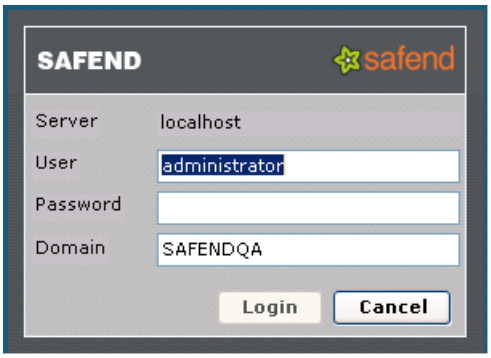
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com


Safend Data Protection Suite Management Console
Welcome to the Safend Data Protection Suite Management Console Setup Wizard
safend
The installer will guide you through the steps required to install Safend Data Protection Suite Management Console on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

2. Proceed with steps 5 through 13 as described above.

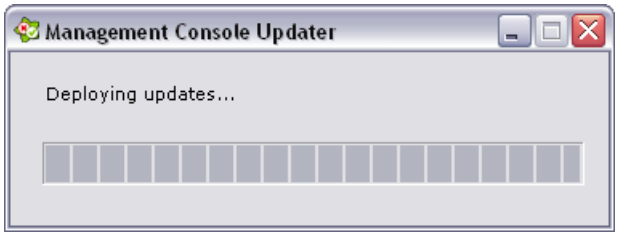
Launching Safend Data Protection Suite Management Console for the First Time

1. Click the icon on your desktop .
   OR
   Go to **Start > Programs > Safend Data Protection Suite > Management Console**. The application opens for the first time:



2. Enter your *User* name, *Password* and *Domain*. The following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



Each time the Management Console connects to the Server, it automatically downloads the latest version of the Management Console (if an update exists). Once the updated files are downloaded, the window closes, and the following window opens:

License Alert - Expiry Warning
- Your Protector: Port and Device Control license will expire in 30 days
- Your Reporter license will expire in 30 days
- Your Removable Media Encryption license will expire in 30 days
- Your Encryptor: Hard Disk Encryption license will expire in 30 days
- Your Inspector: Endpoint Channels license will expire in 30 days
- Your Inspector: Network Channels license will expire in 30 days
- Your Discoverer: Endpoint Data Discovery license will expire in 30 days
Please contact your local reseller or sales@safend.com to purchase a license for this product.
Website: www.safend.com
Support: support@safend.com
View License >>
Enter License Key
Remind Me Later

3. If you are evaluating the software, click **Remind Me Later.**
   OR
   Click **Enter License Key** if you have a valid Safend license, and enter your Safend license key as described in the *Safend Data Protection Suite User Guide, Chapter 11, Administration*.

The Safend Data Protection Suite Management console opens, displaying the main window.

Uninstalling Safend Data Protection Suite Management Console

Here is a description of how to uninstall the console.

➢ To uninstall the Management Console:

1. From the *Control Panel*, open **Add or Remove Programs**.
2. From the list, select **Safend Data Protection Suite Management Console** and click **Remove**.

NOTE

Uninstalling Safend Data Protection Suite Management Console does not cause any information loss. You can re-install it at any time.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Chapter 5

Installing Safend Data Protection Suite Client

About This Chapter

This chapter describes the various methods for installing, or deploying, Safend Data Protection Suite Client. It also explains how to uninstall and upgrade Safend Data Protection Suite Client. It contains the following sections:

- ✓ ***Prerequisites***, page 50, describes the prerequisites of the Safend Data Protection Suite Client.
- ✓ ***Before Deploying Safend Data Protection Suite Client***, page 50, describes the steps you need to take before installing Safend Data Protection Suite Clients.
- ✓ ***Installing Safend Data Protection Suite Client***, page 52, describes the following installation methods:
  - Automatic Client Installation (through Active Directory)
  - Automatic Client Installation (generic)
  - Manual Installation
- ✓ ***Upgrading Safend Data Protection Suite Client*****,** page 61**,** describes how to upgrade the Safend Data Protection Suite Client.
- ✓ ***Uninstalling Safend Data Protection Suite Client***, Page 62, describes how to uninstall Safend Data Protection Suite Client.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Prerequisites

NOTE

Refer to the *What's New* document for the most up-to-date system requirements.

Before Deploying Safend Data Protection Suite Client

In order to install Safend Data Protection Suite Client, you must first install the Management Server. This is necessary in order to raise the security level of the system, by "imprinting" each installed client with the encryption keys of the server. From the point of installation, Safend Data Protection Suite Client knows the keys which it uses when communicating with the Server. From this point on, the Client will not accept any policy or perform any communication with a Server that does not hold matching keys.

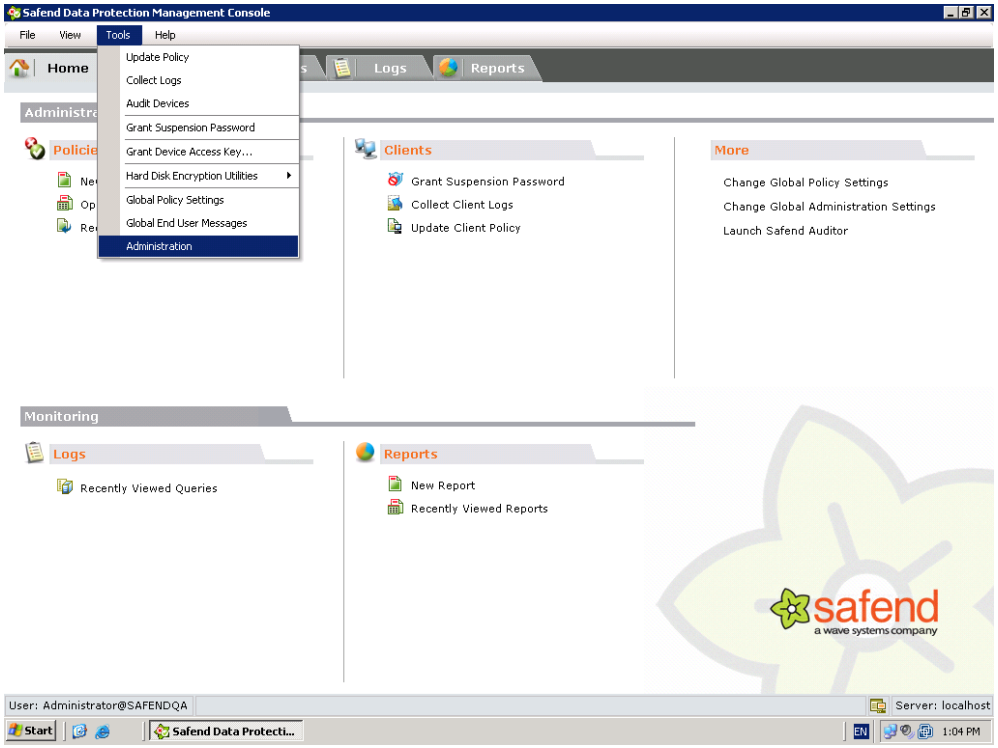
This "imprinting" process is performed by initializing the Client with a file called ClientConfig.scc. This file is generated by the Server upon user request. This file should be available during Client installation.

Before you can start deploying Safend Data Protection Suite Clients you need to define the path to which the Server will generate all the files needed for Client installation. The process of generating the installation files may be performed again at any time.

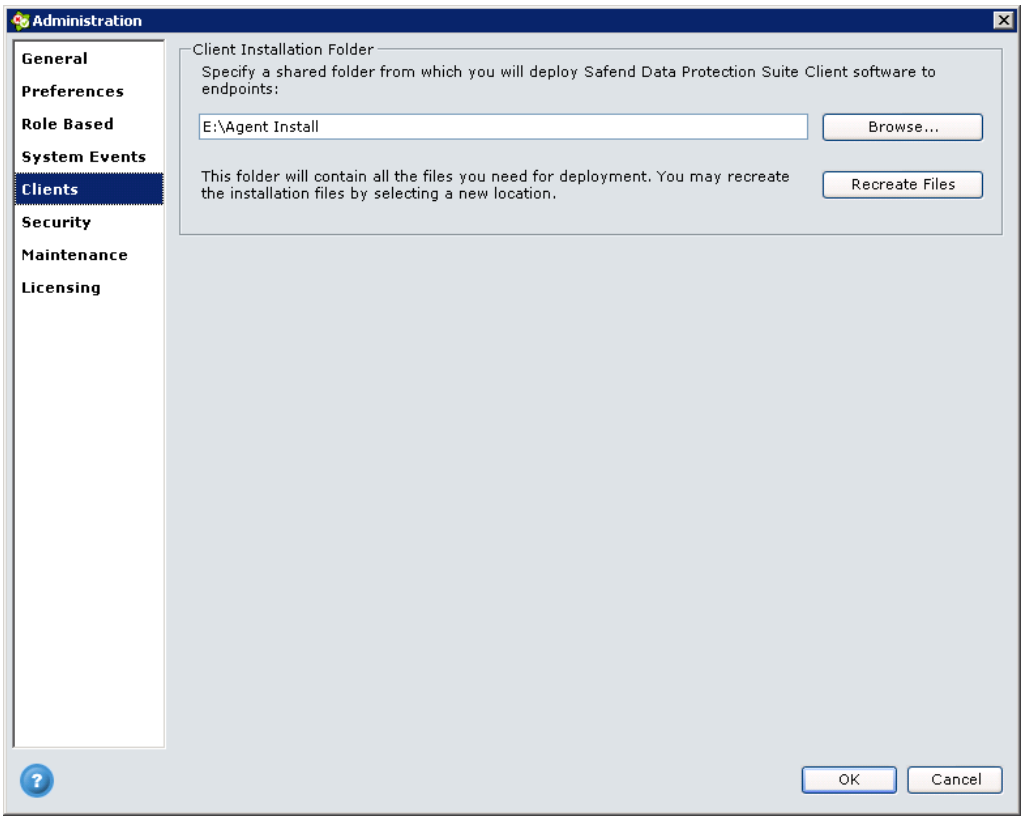
➢ To generate Safend Data Protection Suite Client installation files:

1. In the Management Console, from the *Tools* menu, open the *Administration* window as shown in the following figure:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

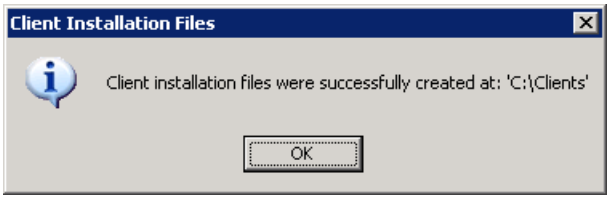


2. In the *Administration* window that opens, click the **Clients** tab on the left. The *Administration>Clients* window opens:



Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

3. Select a shared folder as the Client installation folder. Once the files are created, the following message appears:



IMPORTANT

Make sure you enter a network path and not a local path.

4. Click **OK.**

5. You are now ready to deploy Safend Data Protection Suite Clients on the computers in your organization. Once Clients have been deployed, you can distribute policies to them as described in the *Safend Data Protection Suite User Guide*.

Installing Safend Data Protection Suite Client

There are three ways to install the Safend Data Protection Suite Client:

1. Automatically through the Active Directory Group Policy Management. See *Automatic Client Installation (Active Directory).*
2. Automatically using any corporate software deployment tool, such as SMS and Tivoli. See *Automatic Client Installation (Generic).*
3. Manually by running the installation wizard on each computer. See *Manual Client Installation*.

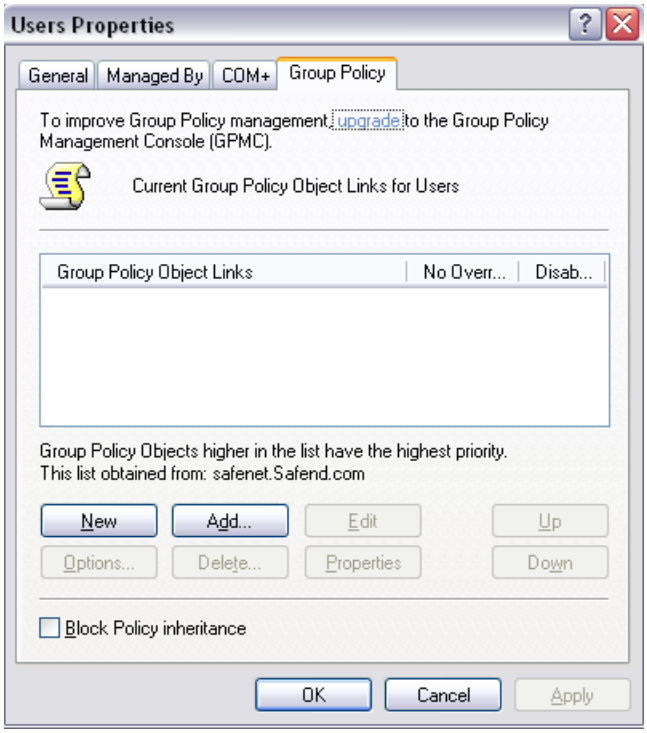
Automatic Client Installation (Active Directory)

Automatic Safend Data Protection Suite Client installation is performed using Active Directory's *Group Policy Management* (if installed) and Active Directory's *Users and Computers*. These options enable you to define a GPO that will distribute the Safend Data Protection Suite Client to the OUs (computer or user groups) of your choice. When this option is used, the clients are installed in Silent mode.

➢ To automatically install the Safend Data Protection Suite Client:

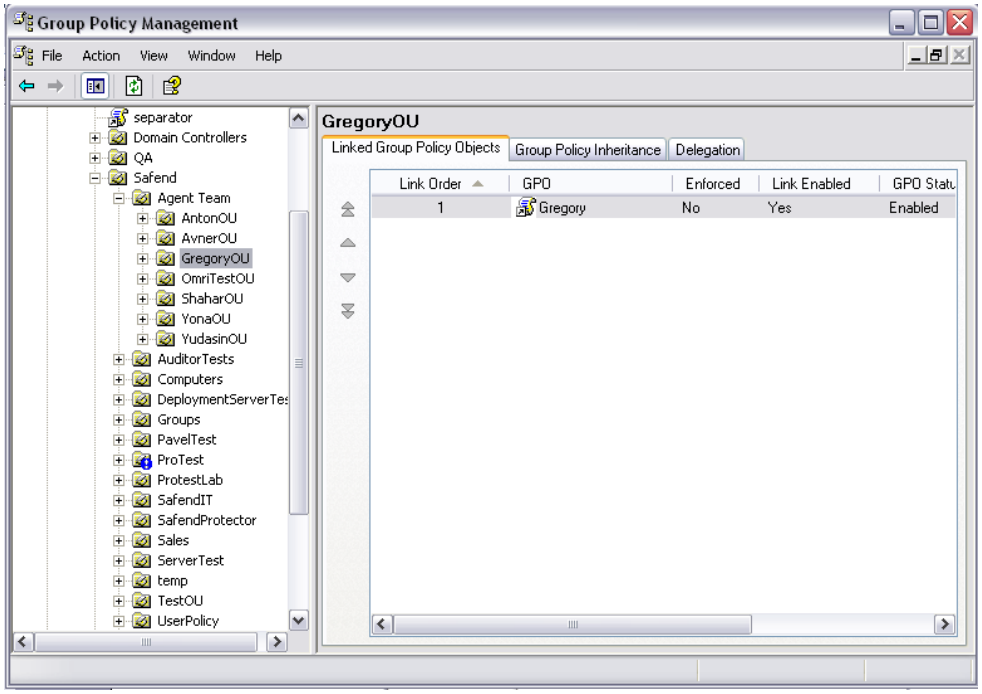
1. Open the Active Directory Users and Computers window.
2. Right-click the OU to which to install the Safend Data Protection Suite Client and select **Properties**. The *User Properties* window opens.
3. In the *User Properties* window, select the *Group Policy* tab. This tab looks different depending on whether the *Group Policy Management Console* is installed or not.
4. If the *Group Policy Management Console* is not installed, the following window is displayed:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



5. Click **New** to add the Safend Data Protection Suite deployment GPO, name it, then right-click that GPO and select **Edit**. Go to *Step 9* below.

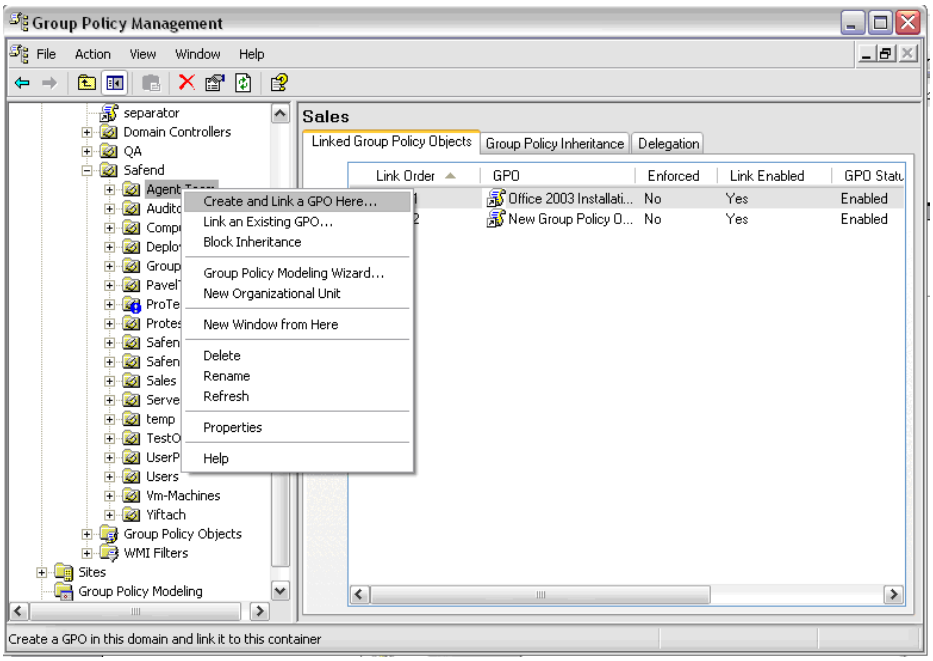
6. If the Group Policy Management console is installed, click **Open** in the *Group Policy* tab to display the *Group Policy Management* window, as shown below:



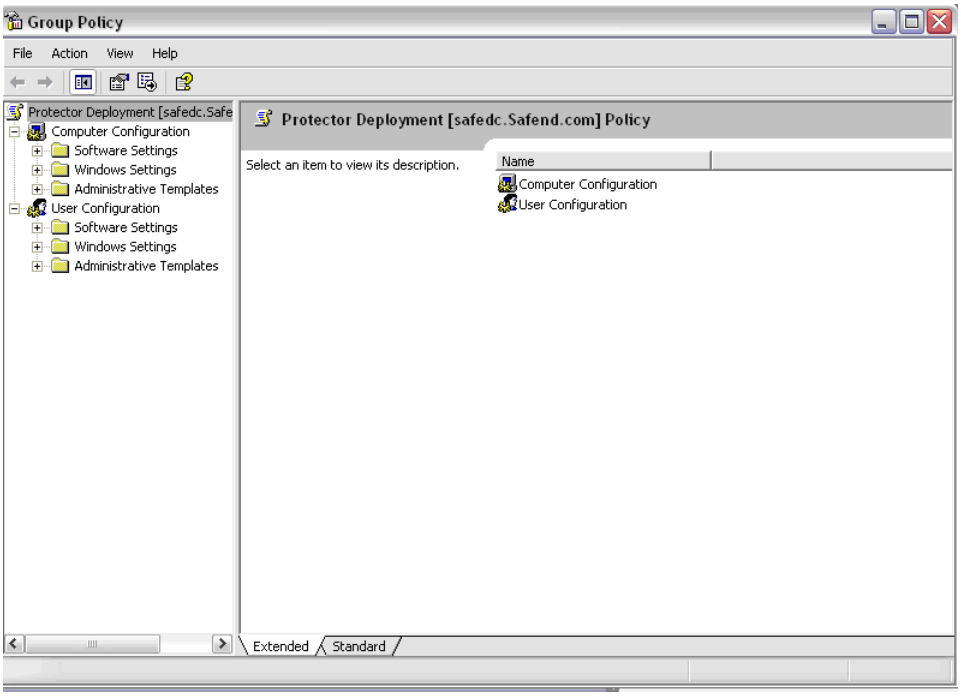
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

7. In the OU tree displayed in the left pane, select the OU to which to install the Safend Data Protection Suite Client. The right pane displays the GPO's that are already assigned to this OU.

8. Add a GPO that installs software to this OU. Right-click on the OU and select Create and Link a GPO Here, then name the GPO.

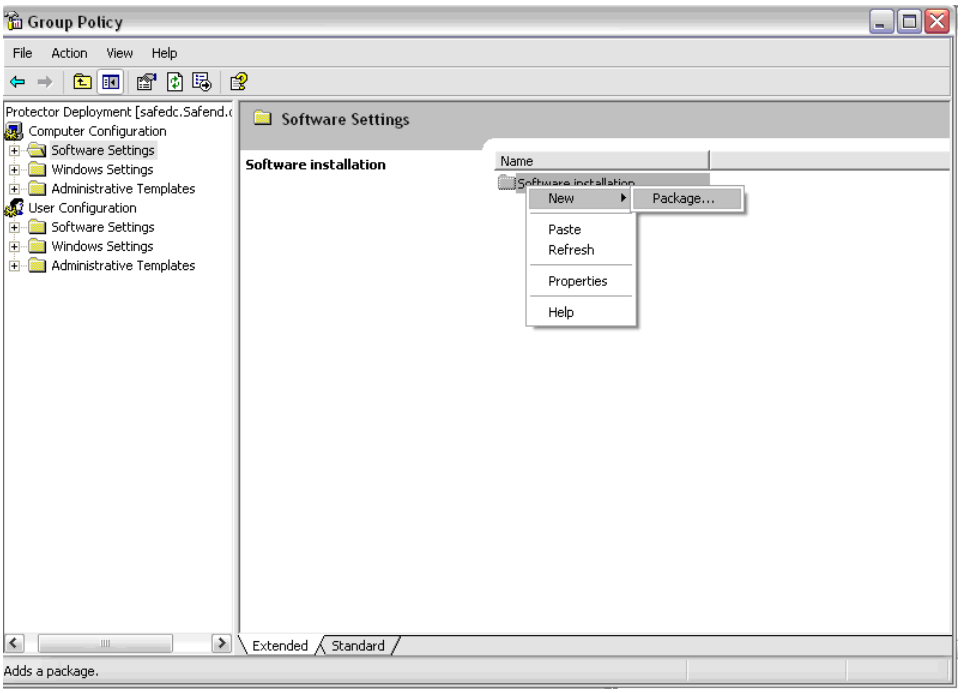


9. Right-click the Safend Data Protection Suite deployment GPO and select **Edit**. The *Group Policy* window is displayed. An example is shown below:



Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

10. Under **Computer** Configuration in the tree on the left, right-click **Software Settings** and select **New**. Then select **Package**, as shown below (the right pane may display names of other software to be installed if any have been defined):

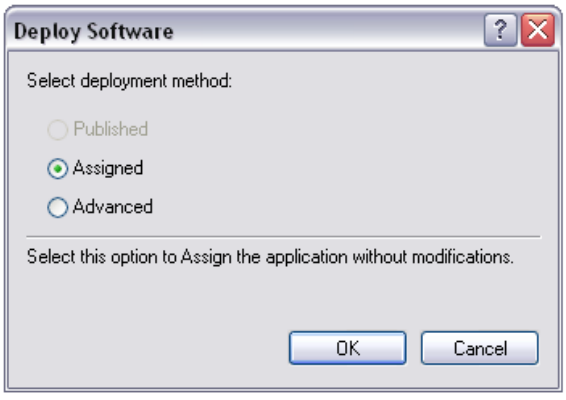


A file selection window is displayed.

11. Locate the shared folder in which you have selected the Client installation files to be created. This folder should contain both the DataProtectionAgent.msi and ClientConfig.scc files.

12. Browse to the full UNC path of the Safend Data Protection Suite Client installation file named DataProtectionAgent.msi, select it and click Open. Make sure this path includes the ClientConfig.scc file.

13. Double-click the **DataProtectionAgent.msi** file. The following window opens:



14. Select Assigned and click OK. Wait a few moments while the MSI is added.

15. Prepare the endpoints of your organization for automatic installation, as described in the *Preparing an Endpoint for Automatic Installation* section below.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

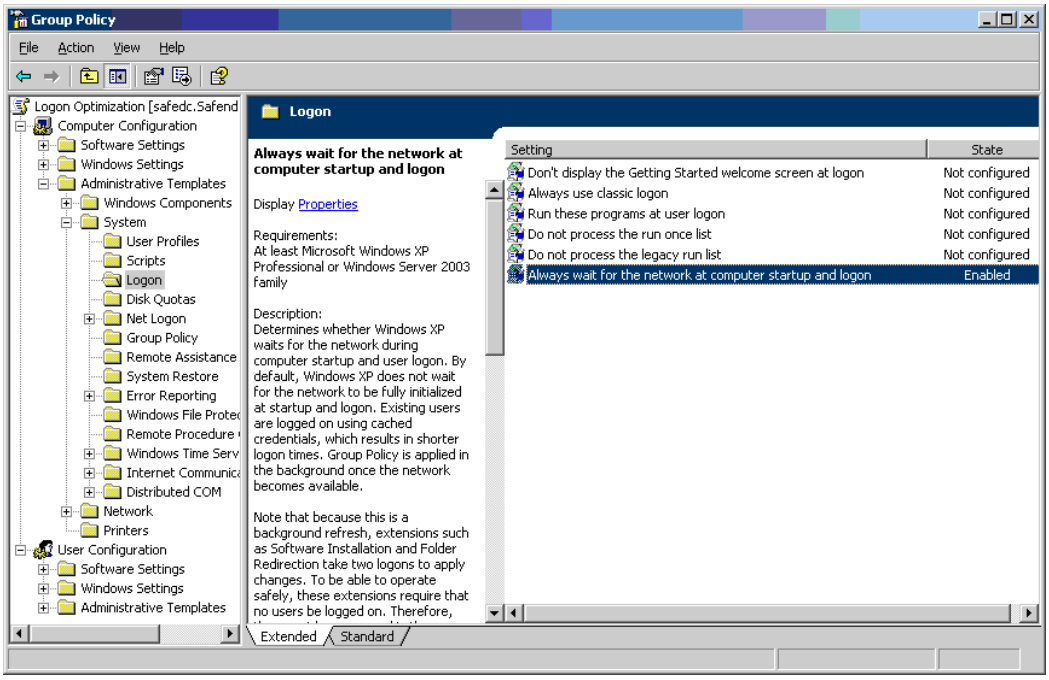
16. A restart will be required on the endpoint computer. A message requiring reboot will be displayed to the end user. To prevent the reboot request from being displayed, please refer to *Automatic Client Installation (Generic).*

NOTE

After the GPO is applied and the computer is restarted, it is possible that the computer will only receive the settings in the GPO upon the restart and a second restart will be required for the settings to take effect (i.e., for the msi to be installed).

Preparing an Endpoint for Automatic Installation

In order to install the Safend Data Protection Suite Client, the target computers are required to have access to the shared network folder when the system is rebooted. If the target computers are running Windows XP, you must turn on the **Always wait for the network at computer startup and logon** GPO, which can be found under **`Computer Configuration\Administrative Templates\System\Logon.`**


Group Policy
File Action View Help
Logon Optimization [safedc.Safend
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Components
System
User Profiles
Scripts
Logon
Disk Quotas
Net Logon
Group Policy
Remote Assistance
System Restore
Error Reporting
Network
Printers
User Configuration
Software Settings
Windows Settings
Administrative Templates
Logon
Always wait for the network at computer startup and logon
Display Properties
Requirements:
At least Microsoft Windows XP Professional or Windows Server 2003 family
Description:
Determines whether Windows XP waits for the network during computer startup and user logon. By default, Windows XP does not wait for the network to be fully initialized at startup and logon. Existing users are logged on using cached credentials, which results in shorter logon times. Group Policy is applied in the background once the network becomes available.
Note that because this is a background refresh, extensions such as Software Installation and Folder Redirection take two logons to apply changes. To be able to operate safely, these extensions require that no users be logged on. Therefore,
Setting
State
Don't display the Getting Started welcome screen at logon
Not configured
Always use classic logon
Not configured
Run these programs at user logon
Not configured
Do not process the run once list
Not configured
Do not process the legacy run list
Not configured
Always wait for the network at computer startup and logon
Enabled
Extended
Standard

The next time a computer or user in this OU reboots, the Safend Data Protection Suite Client will be deployed to it.

NOTE

In some cases, depending on the Domain configuration, it may take some time for the GPO containing the installation package, which is linked to the dedicated OU, to replicate to other domain controllers (usually up to 15 minutes). This may appear as endpoints that are not installing the Safend Data Protection Suite Clients. In this case it is necessary to wait for the replication to finish before restarting the endpoints for installation.

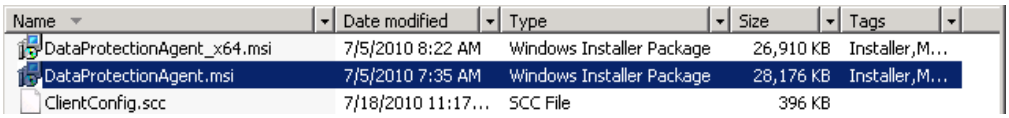
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Automatic Client Installation (Generic)

In order to install using a third-party corporate software management solution, follow the procedure below.

➢ To perform generic automatic client installation:

1. Locate the shared folder in which you have selected the Client installation files to be created. This folder should contain both the *DataProtectionAgent.msi* and *ClientConfig.scc* files. The *DataProtectionAgent_x64.msi* file is also present for machines running 64-bits.



2. Create a batch file containing the following command that installs the Safend Data Protection Suite Client silently:
msiexec /i DriveName:\InstallationPath\DataProtectionAgent.msi /qn

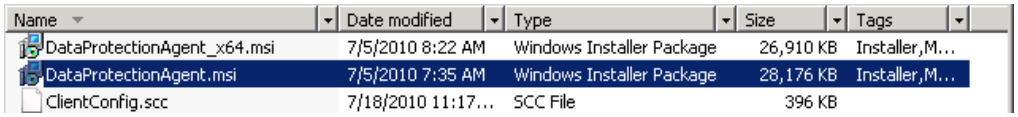
3. A restart will be required on the endpoint computer. A message requiring reboot will be displayed to the end user. To prevent the reboot request from being displayed, add the parameter /norestart REBOOT=ReallySuppress at the end of the command above.

Manual Client Installation

You can manually install the Safend Data Protection Suite Client on each computer in your organization that needs to be protected.

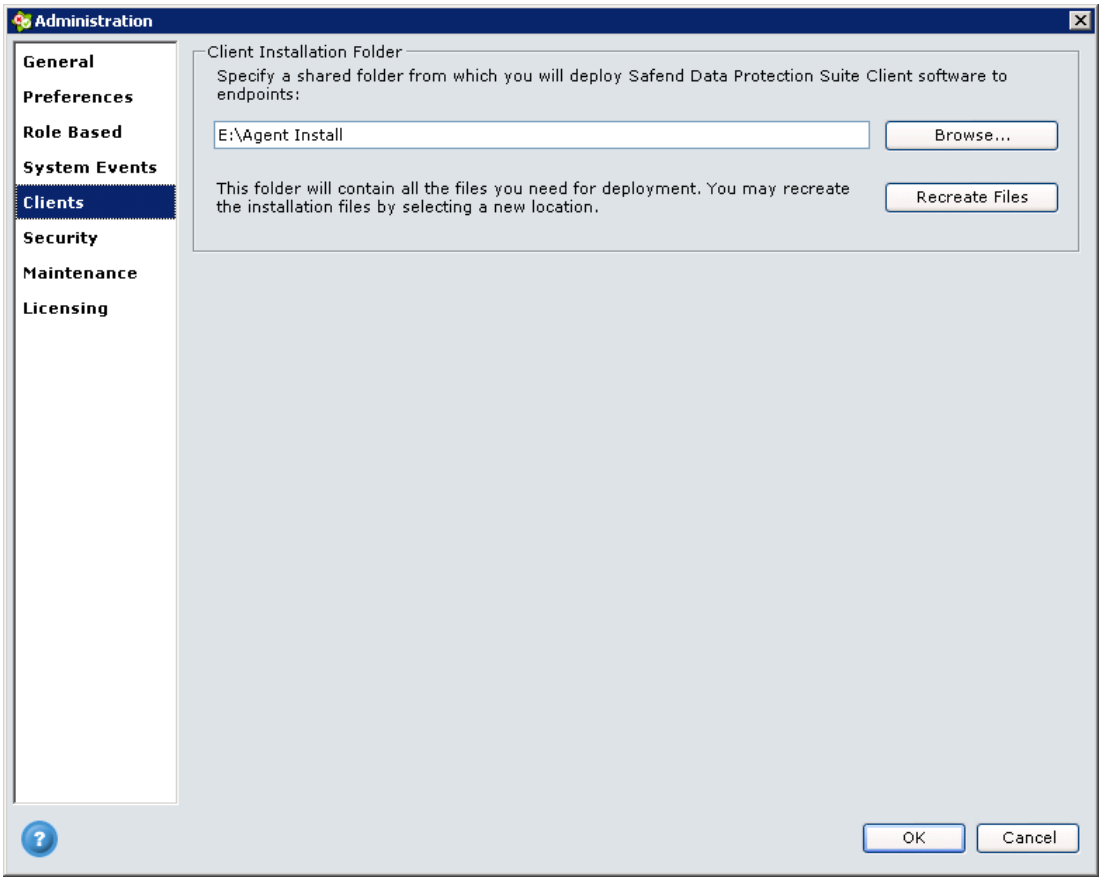
➢ To manually install the Safend Data Protection Suite Client:

1. Locate the shared folder in which you have selected the Safend Data Protection Suite Client installation files to be created. This folder contains the DataProtectionAgent.msi and the ClientConfig.scc files. In order to install the client, both files must be kept in the same folder. The DataProtectionAgent_x64.msi file is also present for machines running 64-bits.

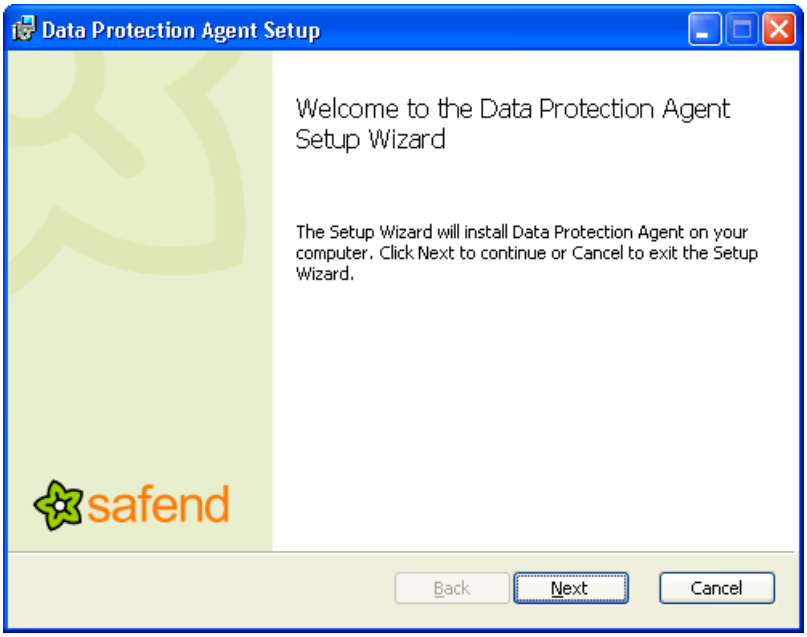


To view the path to this folder, select **Administration** from the Management Console's *Tools* menu, then select the *Clients* tab, as shown in the following figure.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



2. Run **DataProtectionAgent.msi**. If you are deploying clients to a 64 bit machine, make sure you are using the _x64 installer. The installation wizard opens:


Data Protection Agent Setup
Welcome to the Data Protection Agent Setup Wizard
The Setup Wizard will install Data Protection Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
safend
Back
Next
Cancel

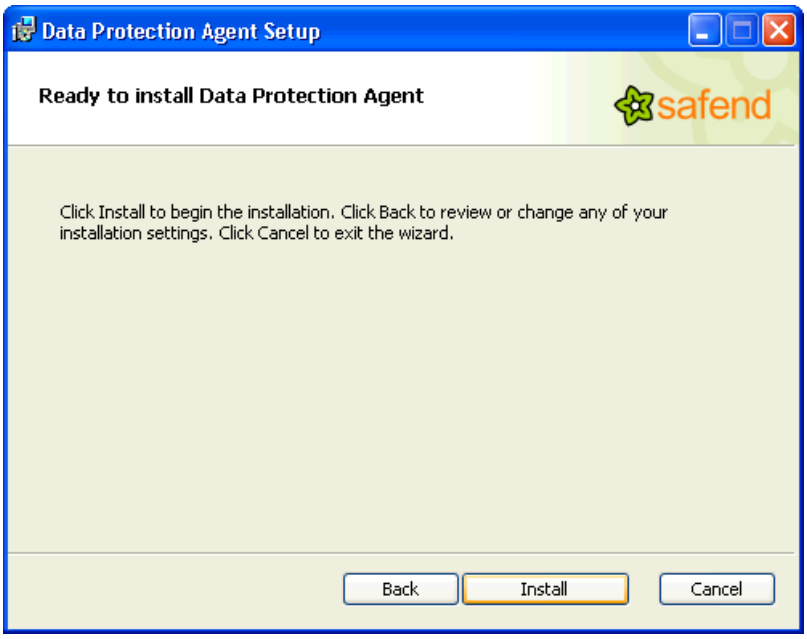
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

3. Click **Next** to continue. The *End User License Agreement* window opens:

Data Protection Agent Setup
End-User License Agreement
Please read the following license agreement carefully
safend
End User License Agreement
PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE CONTAINING SAFEND LTD'S (THE "LICENSOR") PROPRIETARY SAFEND PROTECTOR™ SOFTWARE (THE "SOFTWARE"), AND/OR BEFORE DOWNLOADING/ INSTALLING/USING THE SOFTWARE, AND INDICATE YOUR ACCEPTANCE BY CHOOSING "I
I accept the terms in the License Agreement
Print
Back
Next
Cancel

4. In the *License Agreement* window, select the **I accept the terms in the License Agreement** radio button and click **Next**.

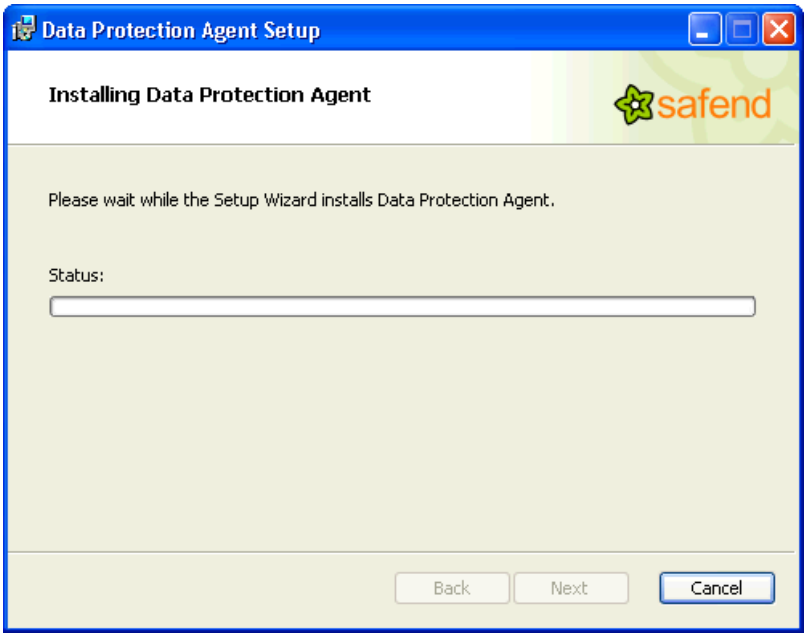
5. The *Ready to Install Data Protection Agent* window opens:


Data Protection Agent Setup
Ready to install Data Protection Agent
safend
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

In this window, click **Back** to review or modify your installation settings, or click **Cancel** to cancel and exit the installation process.

6. Click **Install** to begin the installation. The following window opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

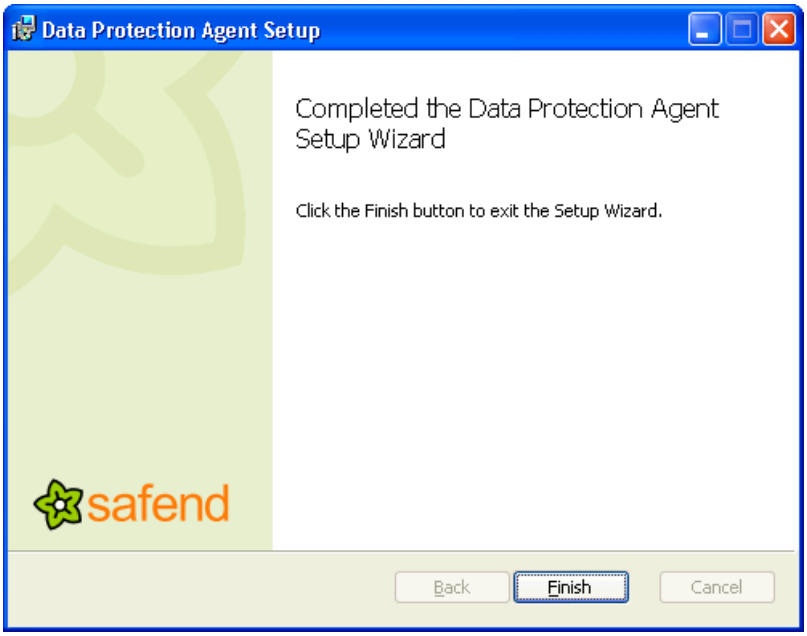


This window contains a Status bar that displays the progress of the installation process. Installation may take several minutes.

NOTE

During this installation, some of the devices attached to your computer may temporarily stop functioning. The devices will resume functioning once the installation has completed.

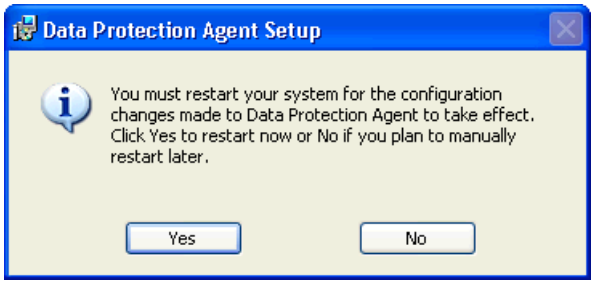
When the installation is complete, the following window opens:



7. Click **Finish** to exit the installation wizard. Safend Data Protection Suite Client is now installed on the endpoint.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

8. You must now restart your computer in order for the Safend Data Protection Suite Client to begin protecting the endpoint. When the following window is displayed, click **Yes**.


Data Protection Agent Setup
You must restart your system for the configuration changes made to Data Protection Agent to take effect. Click Yes to restart now or No if you plan to manually restart later.
Yes
No

Upgrading Safend Data Protection Suite Client

Here is a description of how to upgrade Safend Data Protection Suite clients.

NOTE

Please read *Considerations Before Performing Client Upgrade* before upgrading Clients.

Considerations Before Performing Client Upgrade

- ✓ In case your main objective in performing an upgrade is installing new agents on 64-bit workstations, it is recommended to upgrade the Safend Management Server and install new agents on 64-bit platforms, while keeping the current Safend Agents installed on 32-bit workstations. The new version does not include major changes in the Safend Protector and Safend Encryptor components of the Safend Data Protection Suite, making the agent upgrade in this case redundant.
- ✓ In this version, upgrade and backward computability are supported from Safend Data Protection Suite 3.3 SP7 and up. If you are currently using an older version of Safend Data Protection Suite, or have legacy agents in your environment which were not upgraded yet, it is recommended that you don't perform an upgrade using this version of the Safend Data Protection Suite.
- ✓ Before upgrading Safend Data Protection Agents from 3.3 versions, a preparation action should be performed on the protected machine. The preparation is performed using a lightweight executable that is activated on the protected machine before the upgrade takes place. To obtain the executable, please contact Safend Support.

Upgrading the Client via Active Directory

In order for your endpoint to install the new version of the product, just add the new .msi file as a new GPO (repeat the steps above). This will automatically update the endpoints on the next reboot. Unlike when installing the client, when upgrading do not suppress the automatic reboot which is necessary to complete the upgrade process.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Upgrading the Client Manually

Here is a description of how to upgrade the Client manually.

➢ To upgrade the Client manually:

1. Double-click the **DataProtectionAgent.msi.** Safend Data Protection Suite automatically uninstalls your previous version of the product and updates it with the new version.

4. Following the upgrade, you must reboot the computer on which it was performed (a message will appear requesting you to reboot).

Uninstalling Safend Data Protection Suite Client

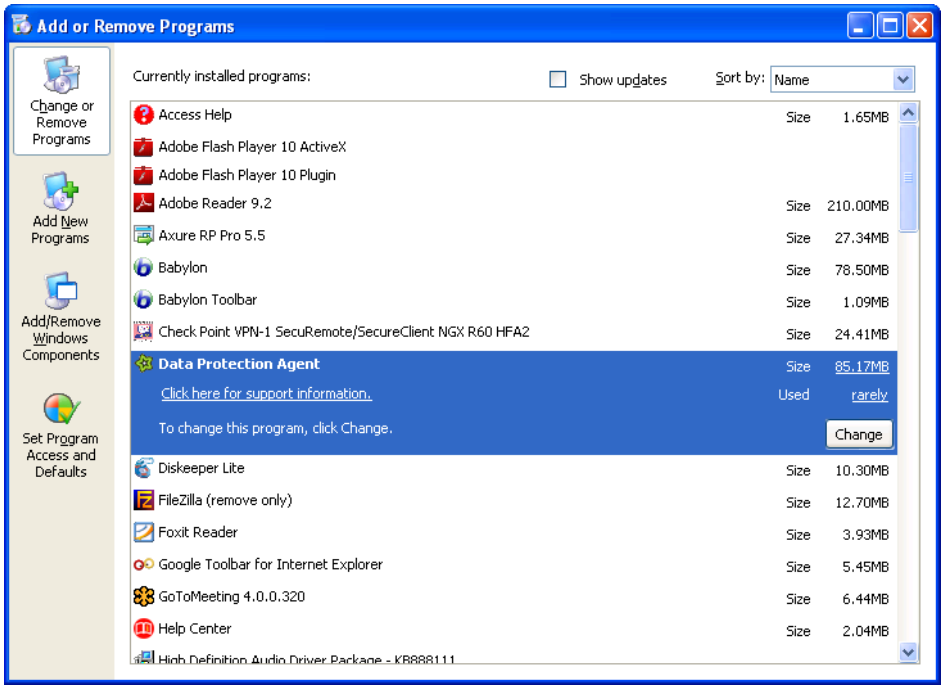
You can uninstall Safend Data Protection Suite either manually, or silently from the GPO. The process of uninstalling is password protected using a global password or a policy-specific password which you defined in the Policies World in the Safend Data Protection Suite Management Console.

Uninstalling Manually

Here is a description of how to uninstall the Client manually.

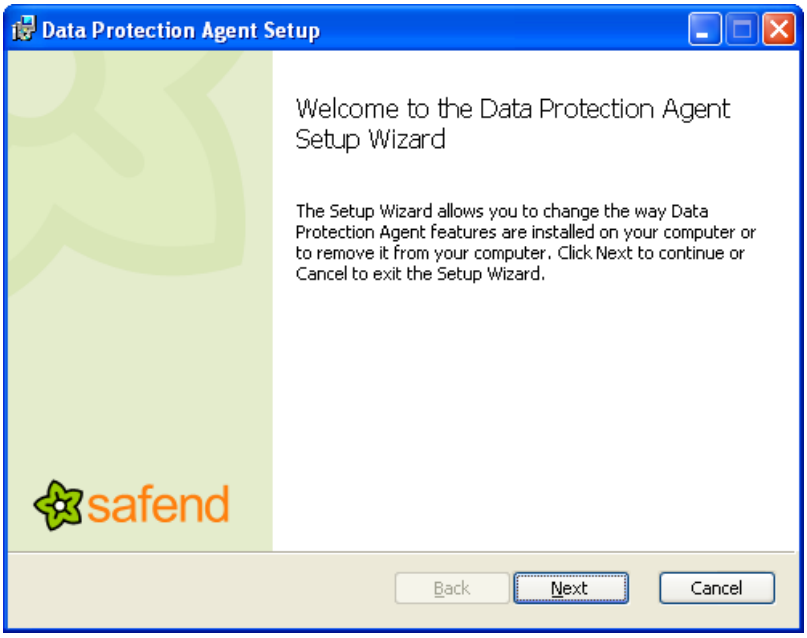
➢ To uninstall manually:

1. From the Control Panel's *Add or Remove Programs*, select **Data Protection Suite Agent** as follows:

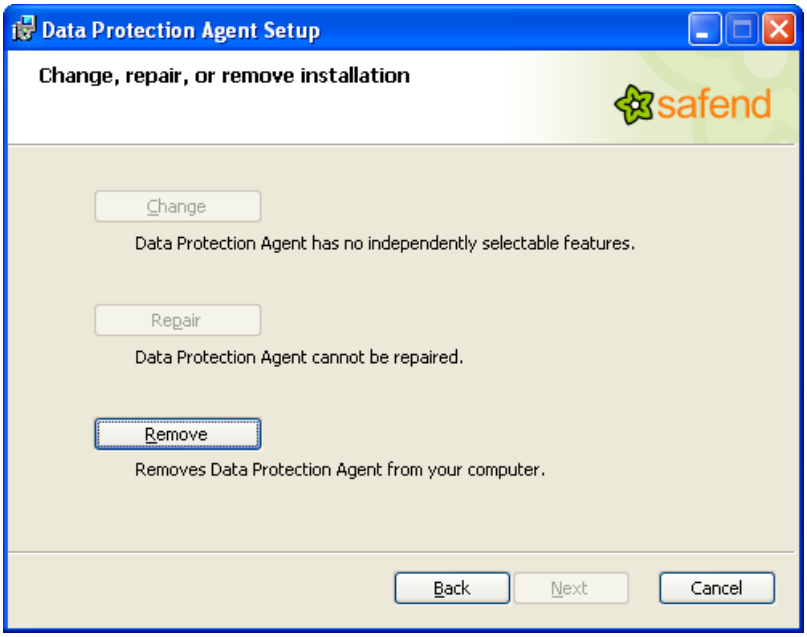


2. Select **Data Protection Agent** and click **Change**. The install wizard opens:

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

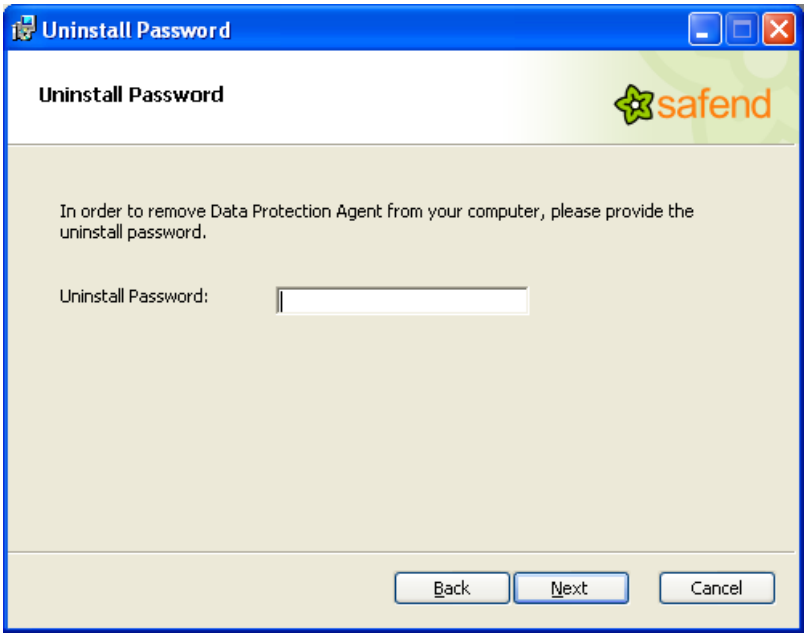

Data Protection Agent Setup
Welcome to the Data Protection Agent Setup Wizard
The Setup Wizard allows you to change the way Data Protection Agent features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.
safend
Back
Next
Cancel

3. Click **Next** to continue uninstalling. The *Change, repair, or remove installation* window opens.



4. Click **Remove** to remove the Data Protection Agent from your computer.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



5. Enter the uninstall password that you defined in the *Policies World* in the Safend Data Protection Suite Management Console and click **Next**. The following window opens:

Data Protection Agent Setup
Ready to remove Data Protection Agent
safend
Click Remove to remove Data Protection Agent from your computer. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Remove
Cancel

6. In order to review or change any settings before continuing, click **Back**, or click **Cancel** to exit the uninstall wizard. Once you have uninstalled it, Safend Data Protection Suite Client will no longer be available to protect the endpoint. Otherwise, continue to the next step.

7. Click **Remove** to remove the Safend Data Protection Suite Client.

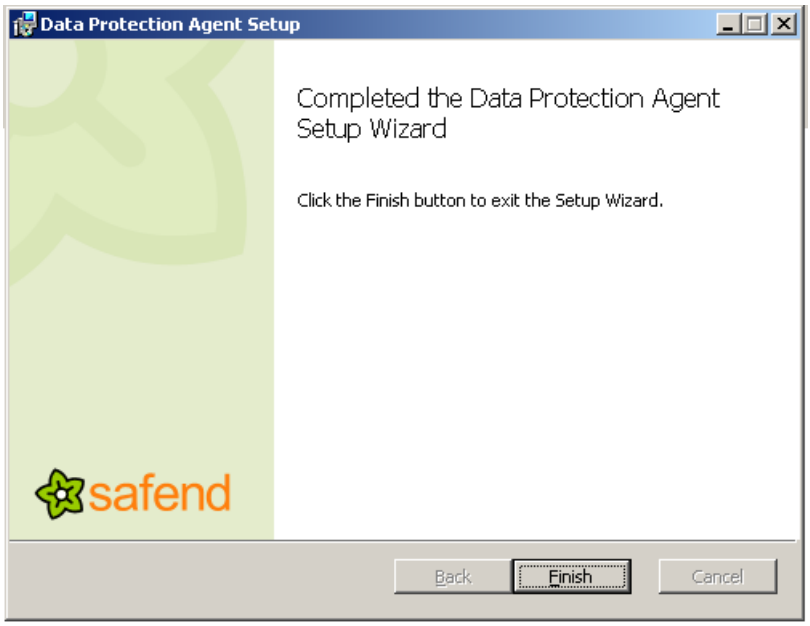
    - When the client has Safend Encryptor add-on enabled, and the hard disk encryption policy is set to encrypt, then an alternate window will appear.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Safend Protector Client - InstallShield Wizard
Remove Hard Disk Encryption
safend
The InstallShield wizard will now be interrupted, and an uninstall process will start removing the Hard Disk Encryption. Once the Hard Disk encryption is removed, the Safend Protector will be automatically uninstalled.
The process might take several hours.
InstallShield
< Back
Remove
Cancel

- Click **Remove** to continue.

The process may take several minutes. When it is completed, the following window appears:



8. Click **Finish**. Safend Data Protection Suite Client is uninstalled and is no longer protecting the computer.

NOTE

After uninstalling you must reboot the computer before you can reinstall Safend Data Protection Suite.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Uninstalling Safend Data Protection Suite via GPO

Since the Safend Data Protection Suite uninstall procedure is password protected, it is not possible to use the automatic uninstall feature in the GPO software installation package. Therefore, to uninstall the Safend Data Protection Suite, a startup script must be used.

There are two ways to uninstall Safend Data Protection Suite Client. The first and recommended option is to unlink the Safend Data Protection Suite Install GPO from the OU containing the client computers, and to apply a **new GPO** containing an uninstall script, as shown in steps 6-11 below. The second option is to edit the Safend Data Protection Suite Deployment GPO.

➢ To uninstall a Safend Data Protection Suite GPO:

1. Edit the relevant Group Policy applied to the client computers from which the Safend Data Protection Suite is to be uninstalled.
2. Navigate to **Computer Configuration > Software Settings >Software Installation**.
3. Right-click the **Safend Data Protection Suite** object and select **All Tasks** > **Remove**.
4. Check the **Allow users to continue to use the software, but prevent new installations** radio button.
5. Click the **OK** button.
6. Create a new GPO Name, *Safend Data Protection Suite Uninstall*, right-click the new GPO and select **Edit**.
7. Navigate to Windows Settings under Computer Configuration and select Script and then Startup.
8. Click the **Show Files** button and create a new text document containing the following command: `msiexec.exe /x` "\\full UNC path to Safend Data Protection Suite shared install folder\DataProtectionAgent.msi" `/qn UNINSTALL_PASSWORD`=uninstall password.

NOTE

The uninstall command set in the batch file (shown above) must be set in one line. The actual uninstall process will take place only after the computer is rebooted. In the case when the endpoint is encrypted, the decryption process will start only after a valid user check-in to the encrypted endpoint.

9. Replace the full UNC path to the Safend Data Protection Suite's shared installation folder with the appropriate path.
10. Replace the uninstall password with the appropriate uninstall password.
11. **Optional**: A restart will be required on the endpoint computer at the end of the uninstall process, and a message requiring reboot will be displayed to the end user. To prevent the reboot request from being displayed, add the parameter /norestart REBOOT=ReallySuppress at the end of the command above.

NOTE

This is only applicable for unencrypted endpoints. If the endpoint is encrypted, then a reboot message will appear after decryption.

12. Save the file with a *.bat extension.
13. Close the folder, click the **Add** button and then the **Browse** button.
14. Select the newly created batch file and click the **OK** button.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Safend Data Protection Suite Client Cleanup Utility

A Client cleanup utility is available for use when you cannot uninstall Safend Data Protection Suite Client from an endpoint, using the processes described above, because the Operating System (OS) is not functioning.

NOTE

In the case where the endpoint is encrypted using internal hard disk encryption, run the Recovery utility. See the *Safend Data Protection Suite User Guide, Appendix A - Safend Recovery Tool for Encrypted Hard Disk*.

➢ To run the Client Cleanup utility:

1. Run the Windows PE operating system from a bootable CD.
2. Run `spec.exe`. The Cleanup Utility window opens.
3. Supply the computer-specific Cleanup Token to Safend support (support@safend.com). Once you receive your cleanup key from Safend support, enter it in the *Cleanup Key* field.
4. Enter the path for the 'system32' operating system folder.
5. Click **Cleanup Now**. The Client cleanup process begins and a progress bar shows its progress. This may take a few minutes. Once cleanup is complete, the following window appears:

6. Restart the endpoint by booting up the OS.
7. Run the Support Assisted Uninstall process to completely remove the agent from the machine.

NOTE

If the internal hard disk was encrypted, after using the Client Cleanup Utility, use the Safend Recovery utility to decrypt the encrypted data. For more information on how to use the Recovery tool, see the *Safend Data Protection Suite User Guide*, *Appendix A - Safend Recovery Tool for Encrypted Hard Disk*.

Emergency Agent Uninstall

A procedure is available to remove the Safend Data Protection Suite Agent when a regular uninstall procedure using an uninstall password is not possible.
This may be necessary in the following instances:

- The agent is properly installed on the machine, but the administrator has forgotten the uninstall password, and the server and all backup files were lost so a new password cannot be set. **Solution:** use Support Assisted Uninstall.
- The administrator has the correct uninstall password, but the agent cannot access the policy in order to verify it, so a regular uninstall cannot be performed. **Solution:** use Support Assisted Uninstall.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

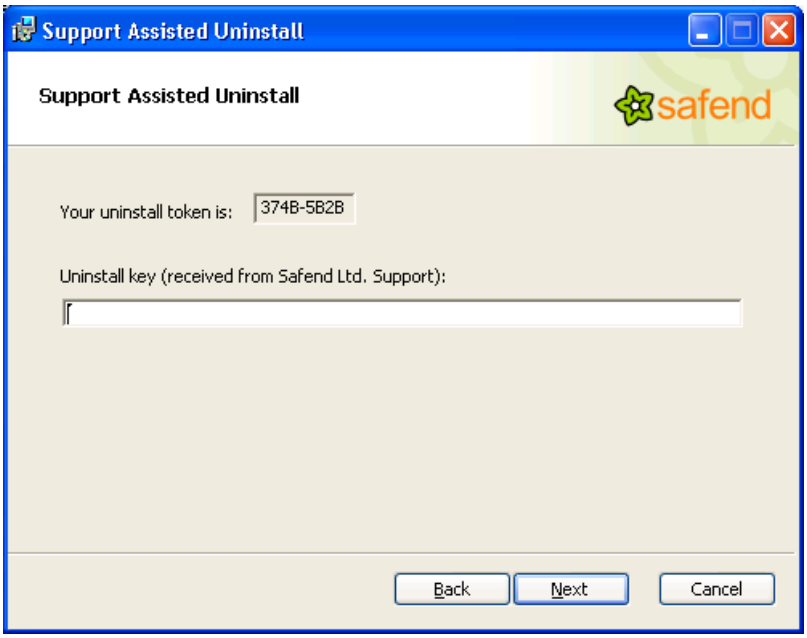
- The OS cannot boot anymore due to a problem with the agent's installation. Solution: run spec.exe on PE and then use Support Assisted Uninstall. Refer to *Safend Data Protection Suite Client Cleanup Utility* for more information.

Support Assisted Uninstall

When the uninstall process is initiated from Control Panel/Add or Remove Programs, the uninstall process is the same as using the uninstall password.
In order to use Support Assisted Uninstall, you must initiate the uninstall process from a command line with the parameter `SAU=1`:
The command should be:

```
Msiexec /i [path to product msi|ProductCode] SAU=1
```

After running this command, the following window is displayed:



Click **Next** to validate the uninstall key. If the key is correct the uninstall process continues (as if the correct password was entered) and removes the corrupted installation.

NOTE

For an encrypted machine, when using the interactive uninstall from the GUI, the flow is exactly the same as when performing an uninstall using an uninstall password. The machine will be decrypted prior to uninstalling the agent.
If you are not checked into the machine, you can use the command line to run a support assisted uninstall process without decrypting the HD, prior to removing the agent from the machine.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Uninstall from a Command Line

The uninstall key can be provided as a command line parameter, in order to support remote/automatic uninstall.
You can use one of the following commands for this purpose:

```
Msiexec /i /qn [path to product msi|ProductCode] SAU=1 SAU_KEY=<token>

Msiexec /x [path to product msi|ProductCode] SAU=1 SAU_KEY=<token>
```


Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Chapter 6

Installing a MAC Client

About This Chapter

This chapter describes the method for installing, a Safend Data Protection Suite Mac Client.

- ✓ ***Prerequisites***, page 71, describes the Safend Data Protection Suite Mac client prerequisites.
- ✓ ***Preparing the Installation Package***, page 71, describes how to prepare the installation package.
- ✓ ***Installing a Safend Data Protection Suite Mac Client***, page 71, describes the client installation process for a Mac.
- ✓ ***Uninstalling a Safend Data Protection Suite Mac Client*** page 76 describes how to uninstall a Mac client.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

Prerequisites

NOTE

Refer to the What's *New* document for the most up-to-date system requirements.

Preparing the Installation Package

Prior to installation, you must place the ClientConfig.scc in the appropriate subfolder of the installation package. This file is generated in Administration>Clients. For more information, refer to *Before Deploying Safend Data Protection Suite Client*.

➢ To prepare the Mac Client installation package:

The full path is: DLPSuite.mpkg/Contents/Resources/SDPAgent.pkg/Contents/Resources.

1. Open the context menu for **DLPSuite.mpkg**. Choose **Show Package Contents**.
2. Double click **Contents** and then **Resources**.
3. Open the context menu for **SDPAgent.pkg**. Choose **Show Package Contents**.
4. Double click **Contents** and then **Resources**.
5. Copy the ClientConfig.scc file to here.

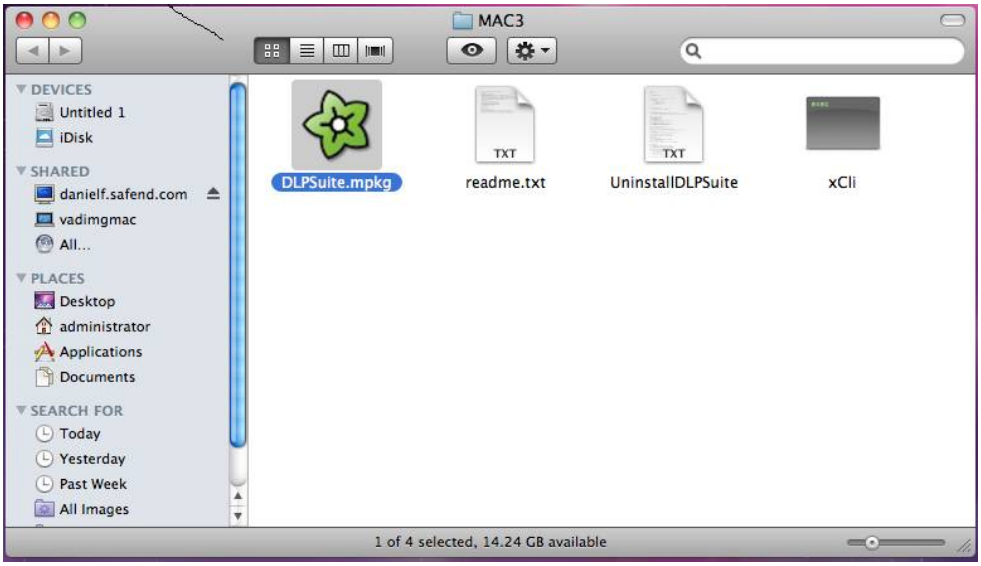
Installing a Safend Data Protection Suite Mac Client

Here is how you manually install the Safend Data Protection Suite Mac Client on each computer in your organization that needs to be protected.

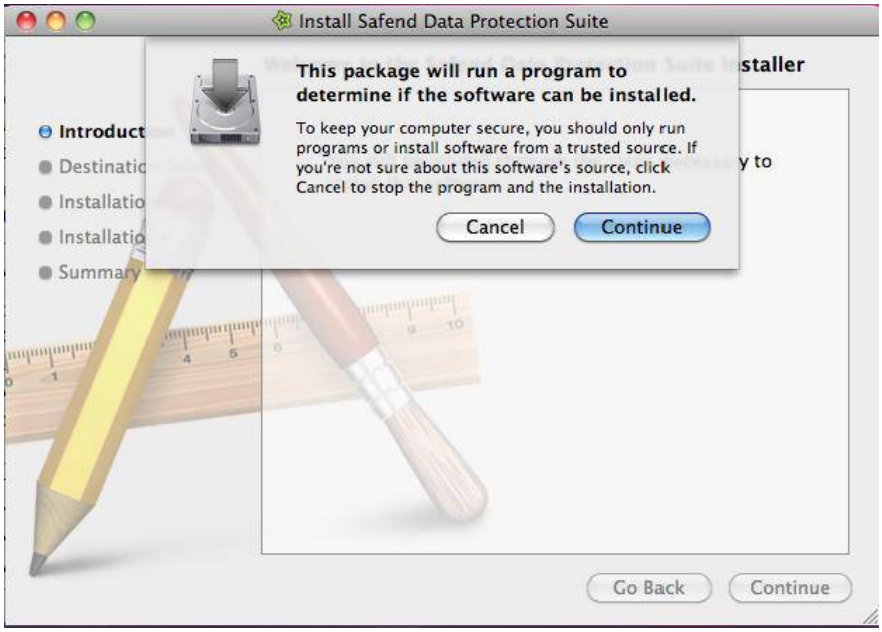
➢ To manually install the Safend Data Protection Suite Mac Client:

1. Run DLPSuite.mpkg.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



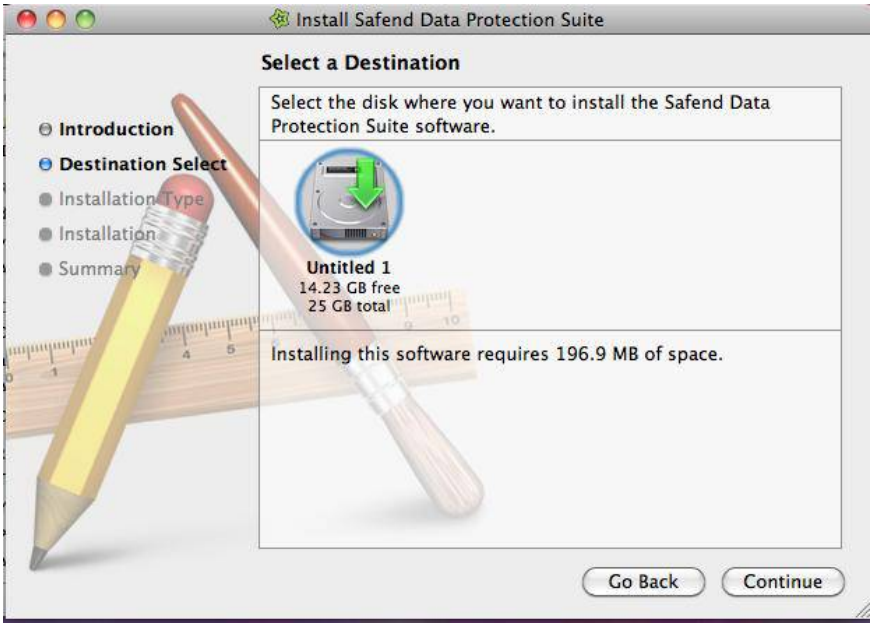
2. Click **Continue.**


Install Safend Data Protection Suite
This package will run a program to determine if the software can be installed.
To keep your computer secure, you should only run programs or install software from a trusted source. If you're not sure about this software's source, click Cancel to stop the program and the installation.
Cancel
Continue
Introduct
Destinatio
Installatio
Installatio
Summary
Go Back
Continue

3. Now the installation configuration process begins, after you click **Continue**.

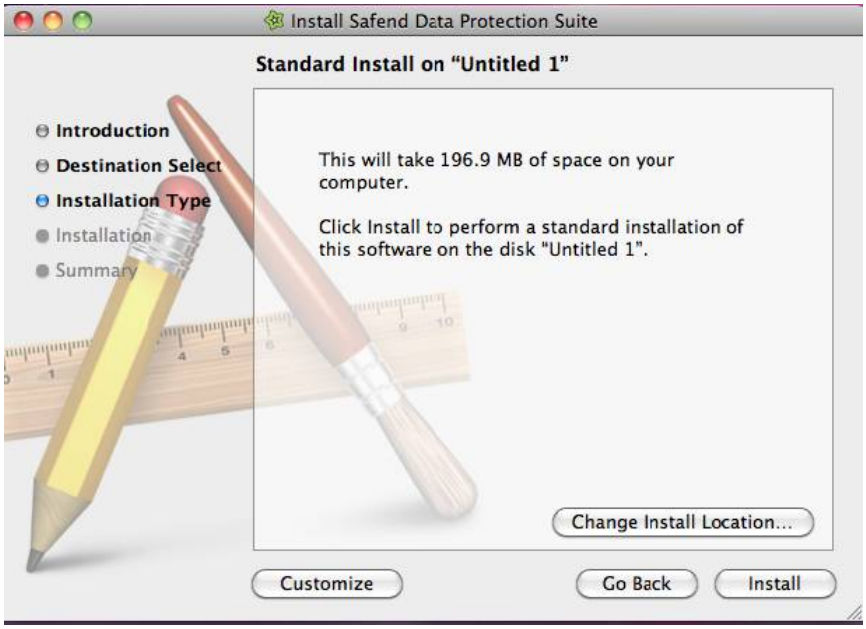
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

4. There is only one option, click **Continue**.



5. Read the summary information and click **Install**.

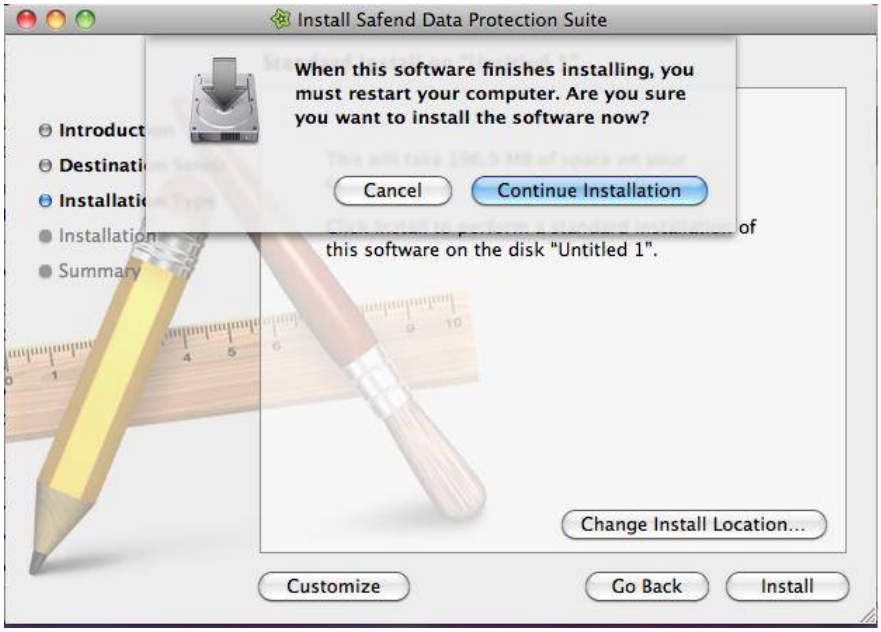
Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



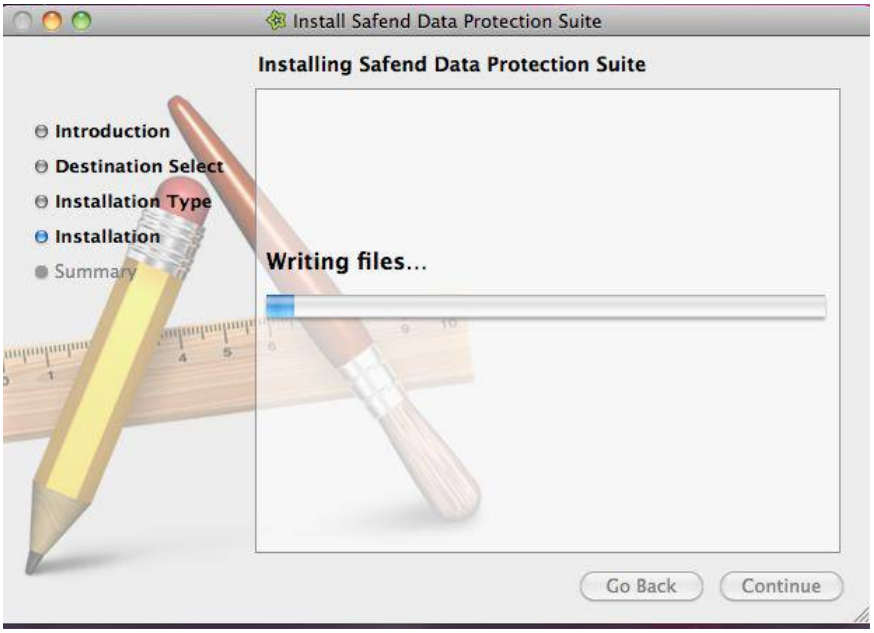
6. Enter the system password.

7. Click **Continue Installation** and the software will now be installed.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com

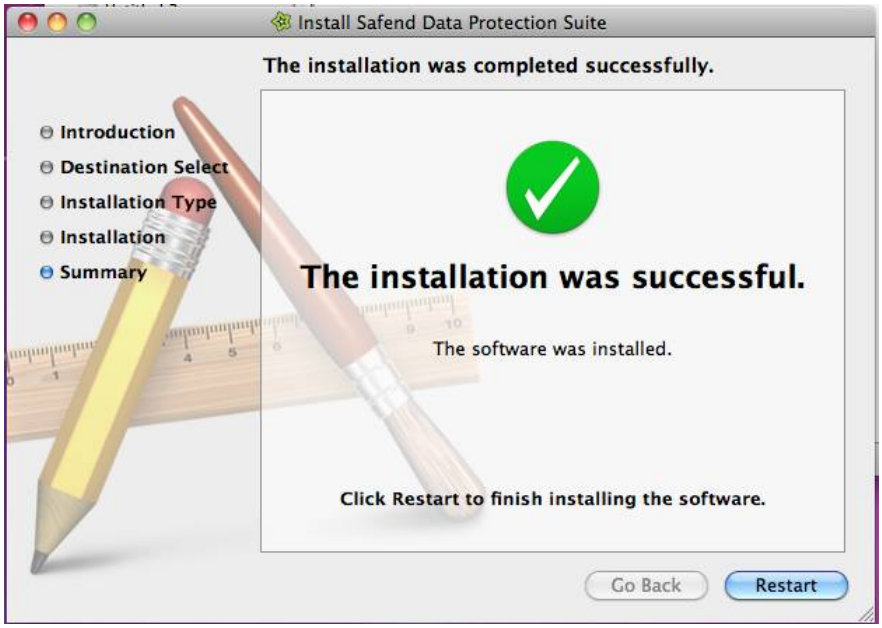


8. You will see the progress bar during the installation process.



9. At the conclusion of the process, you will be informed that the installation was successful. Click **Restart** to reboot the system with the new client.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com



Uninstalling a Safend Data Protection Suite Mac Client

When it is necessary to uninstall a Mac client, follow this procedure.

1. Under the zip file of the Mac Client (available in the FTP from which you downloaded the Server installation package), there is a file namedUninstallDLPSuite.
2. Open the terminal, and run the following: sudo [path to theUninstallDLPSuite file].
3. Enter the administrator password.
4. Reboot the machine once the procedure is completed.

Copyright © 2011 safend a wave systems company | www.safend.com | www.wave.com